BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE INSTRUCTION 33-115, VOLUME 1

24 MAY 2006

Communications and Information

NETWORK OPERATIONS (NETOPS)

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: HQ AFCA/ECF
Supersedes AFI 33-115, Volume 1, 3 May 2004

Certified by: SAF/XCIF (Col Porter Clapp)
Pages: 84

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems* (will become Information Resources Management)**.** This instruction provides the overarching policy, direction, and structure for the Air Force Global Information Grid (AF-GIG) and procedures necessary to manage the increasingly complex network environment. **This instruction applies to the Air National Guard (ANG) and the Air Force Reserve unless indicated otherwise.** Send recommended changes or comments to Headquarters Air Force Communications Agency (HQ AFCA/EASD), 203 West Losey Street, Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF IMT 847, **Recommendation for Change of Publication**, with an information copy to HQ AFCA/ECFP, 203 West Losey Street, Room 2100, Scott AFB IL 62225-5222, and Secretary of the Air Force, Office of Warfighting Integration and Chief Information Officer (SAF/XCIF), 1030 Air Force Pentagon, Washington DC 20330-1030. Major command (MAJCOM) supplements to this AFI will not reduce stated requirements. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records* (will become AFMAN 33-363) and disposed of in accordance with Air Force Records Information Management System (AFRIMS) Records Disposition Schedule (RDS) located at **https://afrims.amc.af.mil/rds_series.cfm**. See **Attachment 1** for a glossary of references and supporting information. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

SUMMARY OF CHANGES

This revision makes this instruction applicable to Air Force Reserve and Air National Guard units at all levels except where explicitly identified. This revision includes office symbol changes and consolidation of the duties and responsibilities of SAF/XCI functions in **Chapter 3**. Air Force Network Operations and Security Center (AFNOSC) roles and responsibilities have been updated in **Chapter 4**. Service Level Agreements have moved to **Chapter 13** and **Chapter 9** has been added which requires use of a maintenance contract and warranty plan; **Chapter 10** addresses vulnerability assessment tools; **Chapter 11** covers Simple Network Management Protocols (SNMP); **Chapter 12** has been added to cover Domain Name

Service Management; **Chapter 13** provides guidance on Service Level Agreements (SLA), and **Chapter 14** covers Records and Forms Management. Other key changes include removing any reference to NOSC-Ds, inserting E-mail updates required by HQ USAF/DP, updating references to field operating agencies (FOA) and direct reporting units (DRU), defining Program Management Office & System Program Office limitations, defining warfighting headquarters (WFHQ) roles and responsibilities, establishing the "edu.af" domain, clarifying the third tier naming structure and removes all references to the Air Force Enterprise Network (AFEN). Additional minor administrative corrections were made and references updated.

Chapter 1

GENERAL INFORMATION

1.1. Background.

1.1.1. This AFI provides the overarching policy, direction, and structure for the Air Force-Global Information Grid (AF-GIG). It is a key component in the efforts to Operationalize and Professionalize the Network (OPTN). The goal of Network Operations (NETOPS) is to provide effective, efficient, secure, and reliable information network services used in critical Department of Defense (DOD) and Air Force communications and information processes. This instruction provides the guidance necessary to manage the increasingly complex network environment and provide customers high quality services. Our networks have evolved into mission critical systems supporting Air Expeditionary Forces (AEF) and joint operations. Continued reliance on information-based weapons systems drives the need for a cohesive Air Force network.

1.1.2. Previously, management of the AF-GIG was centered around the base Network Control Centers (NCC). Today, our goal for managing the AF-GIG is to migrate to a hierarchical environment whereby management of the AF-GIG is distributed across three management tiers (see **Table 2.1.**). This operational concept has evolved over time with the explosive growth and increasing interconnectivity of the many networks and information services that make up the AF-GIG. What is needed is a new way to manage and control the AF-GIG so it can support the increasing demands placed on it by the warfighters, policy makers, and support personnel.

1.2. Air Force Network Operations (AFNETOPS) Scope.

1.2.1. General.

1.2.1.1. Global Information Grid (GIG). The GIG is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve Information Superiority. It also includes National Security Systems (NSS) as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all DOD, national security, and related Intelligence Community missions and functions (strategic, operational, tactical, and business), in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems. It includes any system, equipment, software, or service that meets one or more of the following criteria: transmits information to, receives information from, routes information among, or interchanges information among other equipment, software, and services; provides retention, organization, visualization, information assurance, or disposition of data, information, and/or knowledge received from or transmitted to other equipment, software, and services; processes data or information for use by other equipment, software, or services. (DODD 8100.1, *Global Information Grid (GIG) Overarching Policy*).

1.2.2. Applicability.

1.2.2.1. This instruction applies to the Air Force Total Force which includes HQ USAF, functional communities, MAJCOMs, direct reporting units (DRU), field operating agencies (FOA), Air Force Reserve and ANG. ANG units at all levels except where explicitly identified in the appropriate paragraph will follow this instruction. In all cases ANG personnel who deploy in support of active duty missions will comply with this instruction. This instruction also applies to units and work centers which perform Functional System Administrator (FSA) duties on Air Force systems operated on Air Force networks.

1.2.2.2. The AF-GIG includes any Air Force-provisioned system, equipment, software, or service residing on the Nonsecure Internet Protocol Router Network (NIPRNET), Secret Internet Protocol Router Network (SIPRNET) or ConstellationNet.

1.2.2.2.1. Transmits information to, receives information from, routes information among, or interchanges information with other equipment, software, and/or services.

1.2.2.2.2. Processes data or information for use by other equipment, software, and/or services.

1.2.3. The dynamic and complex nature of the AF-GIG requires an organized management methodology. The Information Technology Infrastructure Library (ITIL) has become the de facto information technology (IT) management standard across both industry worldwide and DOD. This instruction implements guidance that fits into the ITIL. More information about the ITIL can be found at **http://www.ogc.gov.uk/index.asp**.

Chapter 2

NETWORK OPERATIONS HIERARCHY

2.1. Overview.

2.1.1. The Defense Information Infrastructure Control Concept (DIICC) and AFNETOPS Relationship.

2.1.1.1. The AFNETOPS hierarchy adheres to the DIICC. The DIICC consists of three areas of distributed responsibility at global, regional, and local levels. The AFNETOPS relationships and responsibilities span all three levels. However, within the DOD hierarchy, the Air Force Network Operations and Security Centers (AFNOSC) and MAJCOM Network Operations and Security Centers (NOSC) are all considered regional organizations in recognition of Defense Information Systems Agency's (DISA) overarching responsibility for other military services and other DOD agencies. The Air Force NETOPS organizations and their span of responsibilities within the Air Force are depicted in **Table 2.1.**

Table 2.1. Hierarchy of AFNETOPS.

AFNETOPS Level	**Responsible Air Force Organizations**
Global **(Tier 1)**	AFNOSC, DISA's Global NOSC (GNOSC)
Regional **(Tier 2)**	**NOSC, AFRC and ANG NOSC, Functional Awareness Cell (FAC)** **ANG SIPRNET ROSC**
Local **(Tier 3)**	Active Duty, AFRC and ANG NCC, ANG ROSC, NCC-Deployed (NCC-D) SIPRNET System Administrators

2.1.1.2. **Table 2.1.** provides examples of major support activities aligned with each level of the AFNETOPS hierarchy. **Figure 2.1.** depicts the AFNETOPS command relationships between the global, regional, and local levels. The associated Joint, DISA, MAJCOM, and base-level elements are also shown. These relationships are the means for ensuring global systems interoperate without diminishing the authority of local commanders to direct and manage the IT and communications assets under their control. Processes and procedures governing these relationships are meant to be complementary and minimize redundancy.

2.1.1.3. Vice Chief of Staff of the Air Force (VCSAF) message, Command and Control of Air Force Network Operations, dated 3 July 2003, directed the appointment of the Air Force NETOPS Commander as the single Air Force commander responsible for applying network control and defensive measures in a coherent, disciplined fashion to protect the AF-GIG and the advantages it affords to enable Air Force operations.

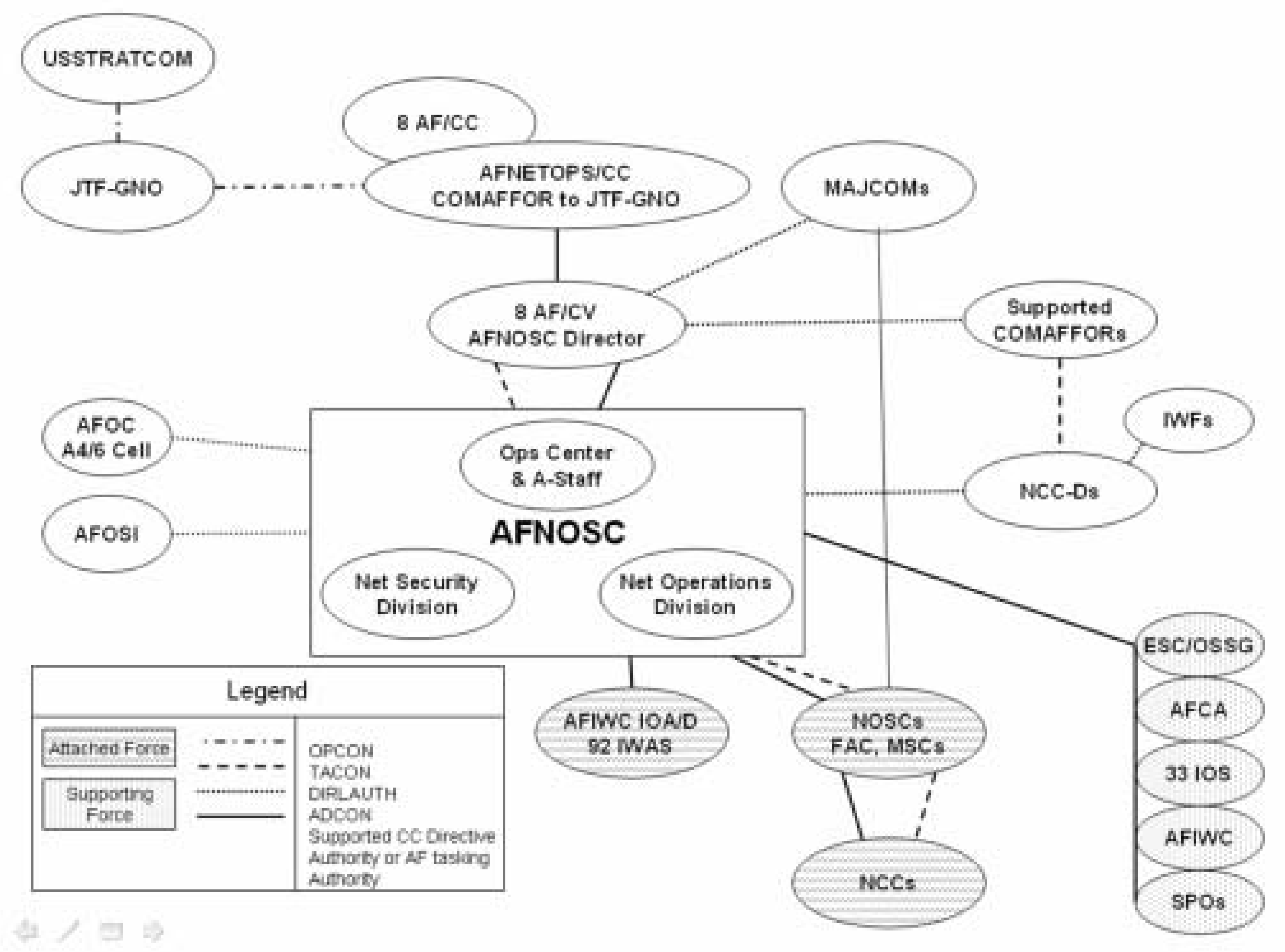
2.1.1.3.1. The AFNETOPS/CC has the authority to implement the Standardization and Evaluation (Stan/Eval) program over the entire AF-GIG, as depicted in **Figure 2.2.** The AFNETOPS/CC will also be authorized Direct Liaison Authority (DIRLAUTH) to MAJCOM SCs and NOSCs. The 8 AF/CC serves as both the AFNETOPS/CC and the Commander of Air Force Forces (COMAFFOR) to the Joint Task Force-Global Network Operations (JTF-GNO) and is responsible for ensuring Air Force forces perform the missions and tasks assigned by the JTF-GNO. The COMAFFOR to JTF-GNO exercises Operational Control (OPCON) over attached units and supported commander directive authority or Air Force tasking authority over supporting forces to implement NETOPS and Network Defense (NetD) actions in support of joint objectives. The AFNETOPS/CC may delegate directive authority to the AFNOSC Director.

2.1.1.4. The 8 AF/CV is also the AFNOSC Director and will be responsible for integrating AFNETOPS and NetD activities across the AF-GIG.

2.1.1.4.1. Under the integrated AFNETOPS/NetD Command and Control (C2) construct, the COMAFFOR to JTF-GNO will have the authority to assign tasks in response to events that cross MAJCOMs, affect the preponderance of the AF-GIG, or are time-critical to assure network availability and security. In general, this will include taskings to direct NOSCs' and NCCs' configuration changes, Information Operations Condition (INFOCON) changes, and changes to security postures. Theater supporting plans will define situations and objectives under which each supported/supporting relationship occurs.

NOTE: ANG units remain under control of their respective state unless activated by the President. Therefore, this must be taken into consideration when executing C2 of the AF-GIG.

Figure 2.1. Air Force Network Operations Command Relationships.

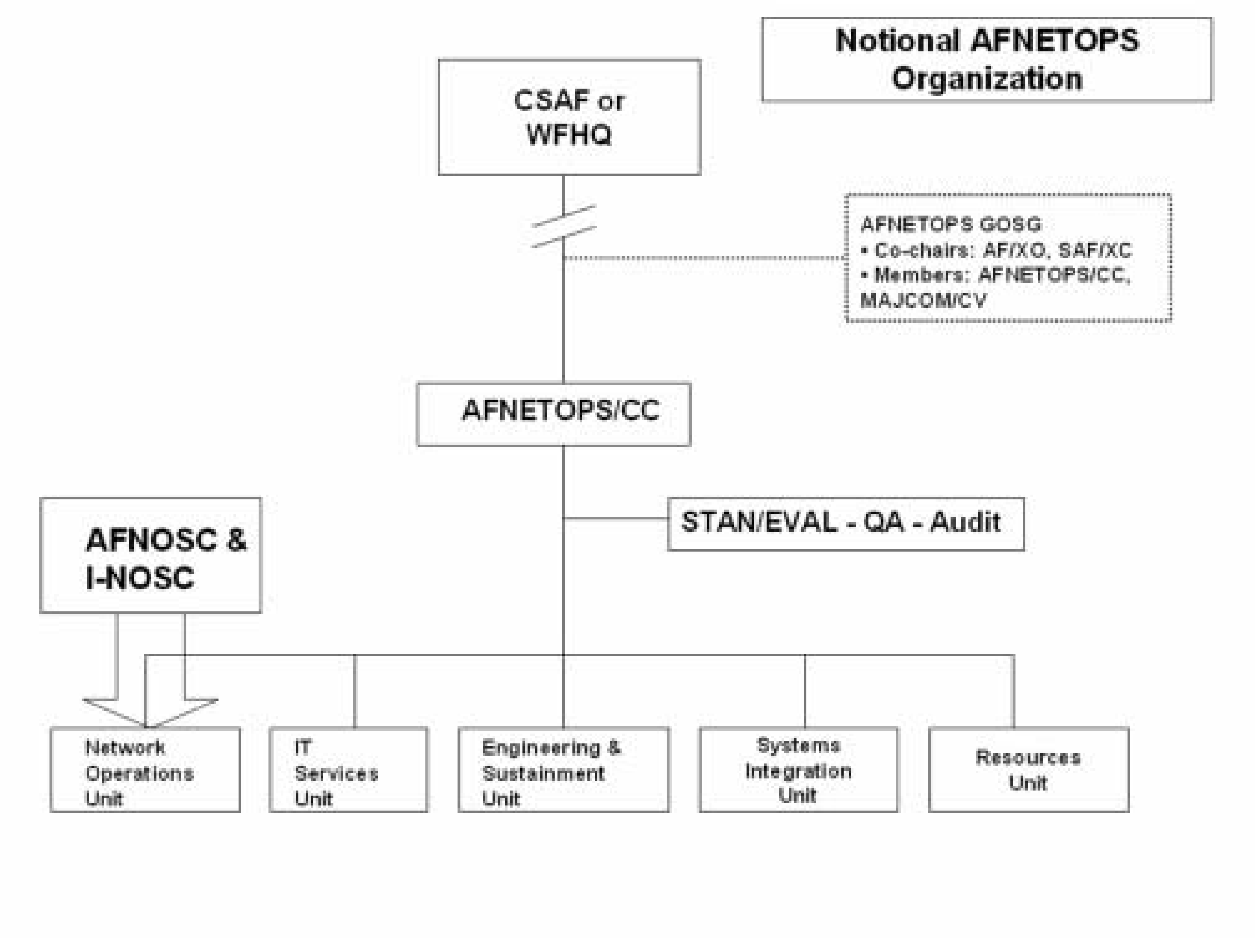


2.1.2. Deployed AFNETOPS Hierarchy.

2.1.2.1. The relationship between the fixed and equivalent deployed AFNETOPS hierarchy is also shown in **Figure 2.1.** The Combatant Command J-6 establishes the Joint Communications Control Center (JCCC) for the JTF AOR, and gives direction through the service's Air Communications Control Center (ACCC). The JCCC does the planning and high-level management of the Joint network and provides specific guidance on Joint circuits.

2.1.2.2. DISA's span of control in the deployed environment extends to the JTF systems control (SYSCON). When deployed, Air Force component ACCC supporting NOSC and NCC-Ds will use the approved joint suite of AFNETOPS tools (e.g., Joint Network Management System [JNMS]) to execute their responsibilities and forward network status to the JTF SYSCON.

Figure 2.2. Notional AFNETOPS Organization.



2.2. Global (DISA/AFNOSC), Regional (NOSC) and Local (NCC) Organizations.

2.2.1. Global.

2.2.1.1. DISA's Global NOSC (GNOSC) is responsible for the worldwide management and operational oversight of the Defense Information Infrastructure (DII). DII network and systems management policy and standards are developed jointly by DISA, the services, and agencies.

2.2.1.2. DISA's span of control ends at the Air Force base network and ANG ROSCs Service Delivery Points (SDP) for fixed communications, and at the Joint SYSCON SDP for deployed operations.

2.2.1.3. All DOD organizations are responsible for complying with the published policies and standards. The NOSCs and NCCs are the primary Air Force organizations responsible for applying and enforcing these policies at the regional and local level.

2.2.1.4. The AFNOSC executes AFNETOPS and NetD through distributed operations. Although elements of the AFNOSC may be physically separated, it will remain one staff under the command and direction of the AFNOSC Director/COMAFFOR to JTF-GNO.

2.2.2. Regional.

2.2.2.1. Regional operation centers depicted in **Table 2.1.** perform NETOPS to ensure operational and administrative control by implementing Systems and Network Management (S&NM), Information Assurance/Network Defense (IA/NetD), and Information Dissemination Management (IDM) within their specific span of responsibilities.

2.2.2.2. The supporting MAJCOM NOSC is responsible for deployed AFNETOPS and reports to the JTF JCCC via the warfighting headquarters (WFHQ) ACCC .

2.2.2.3. Functional Awareness Cells (FAC). These regional level entities exist at the same NETOPS management tier as the Base NCC. They report to and take direction from the Base and supporting NOSC.

2.2.2.3.1. FACs require only a small amount of the equipment and perform situational awareness for a functional system or mission. They act as the point of contact for all computer system trouble calls supporting a particular functional system or group of functional systems. FACs are typically owned and operated by the functional community that the computer system serves. The FAC evaluates problems and typically provides solutions for the application and data associated with that system(s).

2.2.2.3.2. To maintain base network integrity, FACs will not operate their networks, but will operate their own server systems in accordance with Service Level Agreements (SLA), Memorandums of Agreement (MOA), or Memorandums of Understanding (MOU) established with either the NCC or NOSC if an NCC does not exist. The SLA, MOA, or MOU will include how core services (paragraph **6.4.**) are provided by the AFNOSC, NOSC, or NCC so not to jeopardize the integrity of the AF-GIG. See **Attachment 2**, Service Level Agreements, for policy and procedural guidance.

2.2.3. Local.

2.2.3.1. NCCs are the local network control elements through which NOSCs exercise management and operational direction over their MAJCOM network segments. NCCs also generate a situational awareness picture and partner with NOSCs and ANG ROSCs to deliver S&NM, IA/NetD, and IDM. They provide reliable, secure networks, and network services for base-level customers.

2.3. DRU and FOA NOSC realignment.

2.3.1. The 10th Wing and the United States Air Force Academy are aligned to the Air Force Space Command (AFSPC) NOSC.

2.3.2. The Air Force Pentagon Communications Agency (AFPCA) and the 11th Wing are aligned to the Air Mobility Command (AMC) NOSC.

2.3.2.1. All FOAs in the National Capitol region, that are not on Air Force installations, are aligned behind AFPCA as communications geographically separated units (GSU). AFPCA will represent these FOAs to the AMC NOSC. The 70th Wing at Fort Meade is also aligned behind AFPCA.

2.3.3. All DRUs and FOAs on Air Force bases are aligned behind that base NCC and will comply with the “One Base – One Network” guidance.

2.4. NOSC Standardization.

2.4.1. Requirements identified by NOSCs and NCCs that are not addressed by the Combat Information Transport System (CITS) lead command manager or AFI 33-103, *Requirements Development and Processing,* must be approved in accordance with the following process:

2.4.1.1. Requirements must be identified by the MAJCOM and forwarded to the AFNETOPS/CC and SAF/XCIF for validation. (Possible solutions may also be identified.)

2.4.1.2. The AFNETOPS/CC and SAF/XCIF will send validated requirements to CITS Lead Command, HQ AFCA/ECN.

2.4.1.3. AFCA, representing the MAJCOM, SAF/XC and the AFNETOPS/CC, will bring the proposal to the Infrastructure Architecture Council (IAC).

2.4.1.4. If the IAC approves the tool, AFCA will develop a deployment plan and execute the plan under the purview of the AFNOSC and SAF/XC via the CITS program.

2.5. One Base-One Network.

2.5.1. All Air Force units on Air Force installations will comply with the one base-one network philosophy.

2.5.1.1. The base NCC or supporting NOSC will operate, maintain, configure, and control all base core services and network infrastructure.

2.5.1.2. Ownership of all said systems moves to the base NCC and supporting NOSC.

2.5.1.3. All program management office (PMO) and system program office (SPO) systems follow the same above guidance for one base-one network. In special cases, compliance waiver may be requested if funding restrictions prevent corrective actions or the corrections require extensive technical overhaul/analysis. Each exception to policy must include a plan to rectify the issue precluding one base-one network compliance, no waiver will be permanent. Waiver requests must go to AFCA CITS Lead Command for review; then AFCA will forward to SAF/XCIF with recommendations for approval/disapproval.

2.5.2. Geographically Separated Units (GSU).

2.5.2.1. The GSU owning MAJCOM is required to pay for the circuit back to the supporting Air Force base based upon AFI 65-601 Volume 1, *Budget Guidance and Procedures*.

2.5.2.2. The base NCC and supporting NOSC will treat the GSU infrastructure as prescribed in paragraph **2.5.1.**

2.5.2.3. The GSU must be aligned to the base that provides servicing MPF activities for GSU personnel. If they are not currently aligned this way – they must realign appropriately.

2.5.2.4. The GSU will comply with base NCC and supporting NOSC policy, NOTAMs, TCNOs, and other directives as any unit on the base.

2.5.3. Security Enclave Determinations.

2.5.3.1. Units will not define themselves as security enclaves. SAF/XCIF makes the determination as to if a system is to be a security enclave.

2.5.3.2. If a unit wishes to request an enclave determination, submit the request to AFCA for review. AFCA will forward the submission and their review to SAF/XCIF for final disposition.

2.5.3.3. If a unit is declared a security enclave, paragraph **2.5.1.** still applies and the NCC or supporting NOSC will operate all security hardware and core services.

Chapter 3

ORGANIZATIONAL ROLES AND RESPONSIBILITIES

3.1. Secretary of the Air Force, Office of Warfighting Integration and Chief Information Officer (SAF/XC). SAF/XC will:

3.1.1. Develop, validate, and monitor execution of plans, policies, and requirements for modernization of Air Force Communications and Information Infostructure. Provide overall integrated oversight of requirements, plans, schedules, budgets, and performance criteria for all modernization efforts associated with communications and information infostructure.

3.1.2. Lead the development and implementation of communications and information architectures for the Air Force and represent the Air Force position for joint architectures.

3.1.3. Provide policy and guidance for IT registration and administration of the Enterprise Information Technology Data Repository (EITDR) according to AFI 33-202, Volume 1, *Network and Computer Security* (will be incorporated in forthcoming AFI 33-204, *Information Assurance Awareness Program*).

3.1.4. Work with program management offices to ensure all new community of interest systems/servers are developed and implemented with the intent of the CSAF server consolidation effort. Consolidation should start at the DISA Defense Enterprise Computer Center (DECC), however, consolidation to the AFNOSC or NOSC is acceptable as well. Consolidation could include using remote management, co-location, or shared hosting consolidation as best fits the operational mission.

3.1.5. Provide the overarching policy and oversight for all Air Force operational, system, and technical architectures, including establishing IT standards and providing architectural support to the core Air Force processes.

3.1.6. Integrate Air Force planning, budget, financial, and program management processes for IT investments.

3.1.7. Review all 33-series and 37-series AFIs for currency and relevance. The Air Force-Chief Information Officer (AF-CIO) will ensure updates are made and published for all policy documents related to communications and information.

3.1.8. Develop and define the Air Force IT services for the AF-GIG.

3.1.9. Provide oversight of the implementation status of Air Force IT services on behalf of the Secretary of the Air Force (SECAF) and Chief of Staff of the Air Force (CSAF).

3.1.10. Ensure Air Force IT services are in-line with the DOD GIG enterprise services.

3.1.11. Provide oversight of the AF-GIG performance by measurement and analysis of Air Force-level metrics on behalf of the SECAF and CSAF.

3.2. The Deputy Chief of Staff, Air and Space Operations (HQ USAF/XO). HQ USAF/XO is the office of primary responsibility (OPR) for all Air Force information operations matters. Other offices having responsibilities for individual elements affecting NetD will coordinate with HQ USAF/XO to ensure the consistent and standardized application of NetD strategic planning, policy, guidance, and programmatic oversight.

3.3. The Director of Intelligence, Surveillance, and Reconnaissance (HQ USAF/XOI). HQ USAF/XOI is the designated OPR and lead within HQ USAF/XO for coordinating overall NetD policy, guidance, doctrine strategy and investment priorities. Department of the Air Force (Headquarters Air Force, Air Staff and Secretariat) offices with NetD-related responsibilities will coordinate all such matters (to include promulgation of policy and guidance, requirements derivation, and programmatics) with HQ USAF/XOI.

3.4. Information, Services and Integration Directorate (SAF/XCI). SAF/XCI will:

3.4.1. Oversee the day-to-day execution of Air Force communications and information programs, combat support, including wing-level C2, Air Force Forces (AFFOR) C2 and theater level operational support. Develop guidance for command and control, and intelligence, surveillance and reconnaissance networks/nodes.

3.4.2. Develop and articulate positions for communications and information force structure and organizational issues. Analyze proposed MAJCOM force structure and organizational changes and identify impacts on communications and information resources.

3.4.3. Establish course requirements and planning guidance for the professional development, advanced education, and technical training of the communications and information workforce through government and civilian institutions.

3.4.4. Lead career field managers for the communications, information, postal, multimedia, and Communication-Electronic Maintenance (2E) career fields.

3.4.5. Be the lead for communications and information resources (Status of Resources and Training Systems [SORTS], AEF, Unit Type Code [UTC] Functional Area Manager). Determine training requirements and ensure implementation of training programs for assigned Air Force specialties.

3.4.6. Be the lead for establishing an Air Force policy on continuity of operations plans for the AFNOSC, the NOSCs and NCCs.

3.5. Air Force Communications Agency (AFCA). AFCA will:

3.5.1. Conduct network enhancement initiatives. Act as the policy and standards adjunct of SAF/XC. AFCA will administer the OPTN program.

3.5.2. Support SAF/XC by managing the reviews of Information Support Plan (ISP) documents. AFI 33-108, *Compatibility, Interoperability, and Integration of Command, Control, Communications and Computer (C4) Systems* (title will become Interoperability and Supportability of Information Technology and National Security Systems*)* will contain Air Force ISP policy and format guidance when updated.

3.5.3. Address AF-GIG manpower issues. Identify future funding requirements and prepare Program Objective Memorandum (POM) submission in coordination with SAF/XC.

3.5.4. Develop, review, and update Air Force-level SLAs with external agencies as required.

3.5.5. Assist and advise NOSCs and NCCs on optimization of network infrastructures.

3.5.6. Perform Scope EDGE mission. Specifically conduct assessments of base and NOSC network configuration settings for compliance with directives and technical orders. Optimize and secure NOSC and base network configuration settings.

3.5.7. Employ network engineering analysis capabilities to perform quality of service (QoS) analysis for existing warfighter networked systems and applications when these systems and applications do not meet expected QoS.

3.5.8. Provide contract oversight of the Air Force Information Technology E-Learning System (distant learning computer based training), the Books 24x7 on-line reference ware, and the Network Control Center Structured On-the-Job Program for network professionals.

3.6. Air Force Command and Control & Intelligence, Surveillance, and Reconnaissance Center (AFC2ISRC).

3.6.1. Force communications and information workforce are force multipliers which support all six distinctive capabilities the Air Force brings to any activity across the spectrum of military operations, whether as a single Service or in conjunction with other Services in joint operations: Air and Space Superiority, Global Attack, Rapid Global Mobility, Precision Engagement, Information Superiority, and Agile Combat Support. Two of our distinctive capabilities, Precision Engagement and Information Superiority, are information technology driven and information dependent. This is where the communications and information community plays a substantial role. The essence of precision engagement lies in the ability to apply selective force against specific targets and achieve discrete and discriminate effects. Success in doing this means correct use of enormous amounts of information – information that is timely, accurate and useable. Information technology enables us to find, fix, track, and target anything that moves on the surface of the earth. Again, success depends upon a vast amount of the right information, at the right place, at the right time, and in the right format via terrestrial, airborne and space networks seamlessly. AFC2ISRC will:

3.6.2. Review all policy and guidance to ensure network solutions meet warfighter requirements.

3.6.3. Support end-to-end interoperability of network solutions.

3.6.4. Advocate and support appropriate technology and platform implementations.

3.7. Air Force Network Operations and Security Center (AFNOSC). AFNOSC will:

3.7.1. Provide Air Force level C2 and situational awareness for the AF-GIG. Exercise distributed positive control for the classified and unclassified wide area network (WAN) connectivity.

3.7.2. Enforce compliance with accreditation and other network policy.

3.7.3. Develop options and direct configuration changes, INFOCON changes, and changes to security postures in response to vulnerabilities and incidents, JTF-GNO direction, and outages that cross MAJCOMs, affect the preponderance of the AF-GIG, or are time critical in nature.

3.7.4. Issue NETOPS tasking orders (NTO) as well as track, document, and report compliance with Time Compliance Network Orders (TCNO) and C4 Notice to Airmen (NOTAM) provisions of AFI 33-138, *Enterprise Network Operations Notification and Tracking.*

3.7.5. Direct specific actions related to network defense.

3.7.6. Evaluate and respond to Air Force network intrusions and malicious logic events.

3.7.7. Identify Network Attack (NetA) threats by collecting and analyzing intelligence products, and developing and executing countermeasures to network vulnerabilities in coordination with all applicable organizations. Coordinate network restoration after attacks.

3.7.8. Assist NOSCs/NCCs with computer attack damage control and recovery procedures.

3.7.9. Provide top-level tier of technical support for NOSC and NCC WAN operations between SDPs. Technologies and programs to be supported include Domain Name Service (DNS), Air Force Virtual Private Network (VPN), and SDP technology insertion. Specific operational roles and responsibilities are listed in paragraph **4.2.**

3.7.10. Provide senior leaders with global visibility and situational awareness for operational status of AF-GIG resources and capabilities, including NIPRNET, SIPRNET, ConstellationNet and provide information protection related incidents and network outage via Commander’s Situation Report (SITREP) and Operational Reports (OPREP). Maintain awareness of potential or ongoing Combat Air Forces (CAF)/Mobility Air Forces (MAF) operations in order to ensure activities on the AF-GIG do not hinder Air Force operations.

3.7.11. Maintain an enterprise-centric view of the AF-GIG.

3.7.12. Identify and submit network upgrade and operational requirements to Combat Information Transport System (CITS) Lead Command (HQ AFCA/ECN).

3.7.13. Make appropriate joint and Air Force notifications of ongoing or potential NetA activities.

3.7.14. Perform trend analysis and correlation of threat and performance metrics.

3.7.15. Provide command uptime rates for systems and services to include posting uptime rates on a web page.

3.7.16. Establish a Standardization/Evaluation (Stan/Eval) program to encompass the NOSC and NCC operations according to AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals* (will become Network Operations Training and Standards).

3.8. Air Force Information Warfare Center, Information Operations Directorate (AFIWC/IO). AFIWC/IO will:

3.8.1. Maintain and sustain subject matter expertise in Network Defense (NetD) for all networks. Supplement AFNOSC, NOSC and NCC with NetD technical expertise as required for effective response to network attacks. Provide development and employment support for AFIWC developed network sensors and NetD weapons systems (AFIWC/IOD), as well as computer and network threat awareness, analysis, and intelligence support (AFIWC/IOA).

3.8.2. Report to AFNOSCs and MAJCOM NOSCs all backdoors and unauthorized connections to Air Force networks discovered during the course of operations. Reports will be made immediately upon discovery if associated with an on-going incident and within 48 hours from discovery if not associated with an incident response action.

3.8.3. Ensure the 23d Information Operations Squadron develops Tactics, Techniques, and Procedures (TTP) for conducting Information Operations.

3.8.4. Ensure the 92d Information Warfare Aggressor Squadron provides assistance to MAJCOMs by conducting computer and network vulnerability assessments and exercise red team support.

3.8.5. Ensure the 346th Test Squadron conducts formal testing and evaluation of NetD weapon systems, as well as implementation assistance.

3.9. Major Commands (MAJCOM). Each MAJCOM (ANG operates as a MAJCOM) will:

3.9.1. Establish and maintain a NOSC to provide command and control of the MAJCOM network (specific NOSC roles and responsibilities are listed in paragraph **4.3.**).

3.9.2. Develop policies, procedures, and special instructions that pertain to the MAJCOM network.

3.9.3. Identify and submit network upgrade and operational requirements to CITS Lead Command (HQ AFCA/ECN).

3.9.4. Provide network support such as engineering, strategic planning, risk management, developing SLAs, budgeting, inspecting, and contract management to subordinate units. Authorize adequate down time in order to support preventive maintenance inspections.

3.10. Air Education and Training Command (AETC). AETC will:

3.10.1. Manage and provide formal training in support of initial, advanced, supplemental, and qualification training, delivered in-residence and through distance learning.

3.10.2. Identify and submit course resource estimate inputs to the 2E, 3A, 3C, 3V and 33S Career Field Managers for training. Provide oversight of Air Force supplemental technical training. To obtain formal training quotas, refer to Air Force Catalog (AFCAT) 36-2223, *USAF Formal Schools*, and AFI 36-2201, Volume 3, *Air Force Training Program, On the Job Training Administration*.

3.10.3. Identify all training resources required to Career Field Managers.

3.10.4. Plan and program classroom desktop equipment and training aids.

3.10.5. Work, with other MAJCOMs where appropriate, to establish and maintain one “af.edu” domain. Members logged into this domain will not have access to the base infrastructure domain, but, all Air Force members in the .edu domain are required to have “basename.af.mil” E-mail accounts provided by the local base. The purpose of this domain is to establish a unique security enclave conducive to educational exchange and research without exposing the af.mil network to security risks.

3.10.5.1. The AETC NOSC is responsible for the Air Force level functional management of this domain and must work with the other supporting NCCs and MAJCOMs to provide the appropriate level of service.

3.10.5.2. Members of this domain are students and faculty at the United States Air Force Academy, the Air Force Institute of Technology, and the Air University system.

3.10.5.3. The af.edu domain will be its own separate stand alone Active Directory Forrest with independent core services all managed by the AETC NOSC. The infrastructure at each base remains the responsibility of the base NCC and MAJCOM NOSC – this is a logical overlay/separation only.

3.11. Air Force Materiel Command (AFMC). AFMC will:

3.11.1. Provide POM inputs for technical solutions and life-cycle support to AFCA.

3.11.2. Review all TCNO and C4 NOTAMs for applicability to all AFMC provided information systems.

3.12. Wings and Air Base Host Units. Hosting base units will:

3.12.1. Operate and manage NCCs to provide base level network services not managed by NOSC. Specific NCC operational roles and responsibilities are listed in paragraph **4.4.**

3.12.2. Submit networking sustainment and upgrade requirements to their respective MAJCOM or applicable supporting agency for DRUs and FOAs.

3.12.3. Ensure units coordinate with MAJCOMs or applicable agencies for formal training requirements.

3.12.4. Ensure unit commanders appoint 3As as client support administrators (CSA) consistent with paragraph **4.7.**

3.12.5. Grant AFCA Scope EDGE personnel administrative access to base networks to perform compliance assessments and optimization activities, as requested by their parent MAJCOM.

3.13. Air Force Program Management Offices (PMO) and System Program Offices (SPO). PMOs and SPOs will:

3.13.1. Not deliver or operate network infrastructure hardware without IAC approval.

3.13.2. Use base NCC or supporting NOSC provided network services and network core services.

3.13.3. PMO/SPO must comply with one base-one network policy; all systems on the network must be configured to operate within this construct.

3.13.4. Develop Information Support Plans in accordance with Air Force guidance, CJCSI 6212.01D, *Interoperability and Supportability of Information Technology and National Security Systems,* and DODI 4630.8, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),* for any IT or NSS system that exchanges information external to itself, and/or is connected to the GIG.

3.14. Warfighting Headquarters (WFHQ). WFHQ will:

3.14.1. Not operate or maintain network infrastructure hardware or core services.

3.14.2. Use base NCC or supporting NOSC provided network services and network core services.

3.14.3. Provide System Administration support for Air Operations Center delivered C2 systems only.

3.15. Lead Command Managers (LCM). LCMs are:

3.15.1. Responsible for communications and information systems, equipment, commodities or services operated/used by more than one Air Force MAJCOM, DRU or FOA. Lead commands as advocates involves requirements, life-cycle planning, sustainment and resource management and must comply with AFI 10-901, *Lead Operating Command—Communications and Information Systems Management*.

Chapter 4

OPERATIONAL ROLES AND RESPONSIBILITIES

4.1. General. The AFNOSC, NOSC, and NCC are the tiered levels of AF-GIG operations working in concert to ensure networks are available to support mission demands. These centers perform the AF-GIG mission operation areas described in **Chapter 6**. Specific definitions of each tier, as well as roles and responsibilities, are discussed in this chapter.

4.2. Air Force Network Operations and Security Center (AFNOSC). The AFNOSC is the Air Force's top network operations tier. The AFNOSC develops options and directs configuration changes and changes to security postures in response to vulnerabilities and incidents, JTF-GNO direction, and outages that cross theater NOSCs, affect the preponderance of the network, or are time critical in nature. The AFNOSC provides Air Force-level metrics, situational awareness, and enforces compliance with accreditation and other network policy. Although the AFNOSC represents the top tier of the AF-GIG, it does not relieve theater NOSC from managing, resourcing, and implementing the AF-GIG within their respective theaters. The AFNOSC has tactical control (TACON) over the theater NOSC, base NCC and the mission support center (MSC) or FAC to direct configuration changes, INFOCON changes, and changes to the security posture of the AF-GIG. The AFNOSC will:

4.2.1. Operate 24-hours-a-day, 7-days-a-week.

4.2.2. Interact with DISA, JTF-GNO, theater NOSCs, and the commercial sector to identify and correct anomalies in Air Force networks, systems, and applications.

4.2.3. Exercise DIRLAUTH for the Air Force to MAJCOMs, other Air Force agencies, sister services, and other external agencies for network operations and network security issues.

4.2.4. Perform Information Dissemination Management.

4.2.4.1. Issue NTOs as well as track, document, and report compliance with TCNOs according to AFI 33-138, directing all AF-GIG operational, security, and configuration based changes. Ensure two-person compliance procedures are followed according to AFI 33-138 when implementing TCNOs. Issue Air Force-level C4 NOTAMs according to AFI 33-138.

4.2.4.2. Direct all AF-GIG operational, security, and configuration based changes.

4.2.4.3. Draft SITREPs according to AFI 10-206, *Operational Reporting*. Draft Operational Event/Incident Reports (OPREP3) according to AFI 10-206 to document and report significant network events affecting Defense Information Systems Network (DISN) connections not previously reported in SITREPs.

4.2.4.4. Provide Help Desk services to theater NOSCs as a focal point for AF-GIG problem resolution.

4.2.4.5. Document and track trouble calls to final resolution.

4.2.4.6. Utilize Network Common Operating Picture (NETCOP) to consolidate NOSC up-channeled metrics of C4 systems and report overall AF-GIG metrics to SAF/XC, and other senior leaders as required.

4.2.4.7. Monitor and report status and critical metrics of Air Force IT services, as defined by the AF-CIO, NIPRNET, SIPRNET, and JWICS connections to senior leaders and theater NOSC, MSC, FAC, and base NCCs as needed or required.

4.2.4.8. Supply data to program offices, DISA, JTF-GNO, and other agencies, as required, ensuring systemic Air Force-level problem areas are tracked and fixed.

4.2.4.9. Provide status of on-going law enforcement investigations related to computer security incidents to COMAFFOR to JTF-GNO.

4.2.4.10. Report to JTF-GNO COMAFFOR validated NetAs, suspicious activities, and security incidents to DOD CERT, GNOSC, Air Force Office of Special Investigations (AFOSI), Information Warfare Flights, theater NOSCs, NCCs, and other activities, in accordance with DOD and Air Force guidelines.

4.2.5. Perform System and Network Management.

4.2.5.1. Perform continuous voice, video and data network monitoring and analysis of operations for identification of network availability or degradation events.

4.2.5.2. Ensure situational awareness of CITS equipment is maintained and respond/report any system degradation events.

4.2.5.3. Manage Air Force level (af.mil and af.smil.mil) DNS, naming convention for the Air Force, maintain a Name Server (NS) record for all Air Force name servers in the af.mil zone and provide technical support for the af.mil and af.smil.mil domain and sub-domains.

4.2.5.4. Monitor Air Force-level Internet Protocol (IP) address space.

4.2.5.5. Manage the Tactical Internet Protocol (TAC-IP) Program to provide temporary IP address space for deployed units.

4.2.5.6. Administer and maintain Air Force-level system capabilities as negotiated in SLAs.

4.2.5.7. Manage the USAF Circuit Upgrade Program, identify and report circuits that exceed established thresholds to the Air Force Systems Network (AFSN) office.

4.2.6. Perform Information Assurance/Network Defense.

4.2.6.1. Perform continuous network monitoring operations for identification of on-going attacks against the network or interconnected systems.

4.2.6.2. Provide real-time analysis, response and reporting according to AFI 33-138 for network attacks and security incidents.

4.2.6.3. Correlate network events with supporting network data, threat data, and technical vulnerability information.

4.2.6.4. Maintain global situational awareness of events threatening Air Force networks.

4.2.6.5. Manage Air Force long-haul user VPN.

4.2.6.6. Maintain secure communications with NOSCs.

4.2.6.7. Update Access Control Lists on SDP routers.

4.2.6.8. Analyze NETOPS security posture using security management software tools such as intrusion detection and vulnerability assessment.

4.2.6.9. Analyze customer impact of all network incidents, problems and alerts, and develop corrective actions or management changes.

4.2.6.10. Require network defense countermeasures and other defensive or corrective actions in response to command direction, INFOCONs, or vulnerability alerts.

4.2.6.11. Develop and/or exercise contingency plans to continue operations in at least one location in the local area and at least one location outside the local area in the event of natural or unnatural disaster, utilities failure, and contractor issues.

4.2.6.12. Conduct NetA assessments, correlate incidents, conduct spot check compliance, and conduct on-line surveys for suspicious activities (internal and external) across Air Force network domains. Notify COMAFFOR and the JTF-GNO of attacks and suspicious activities. Conduct trend analysis to determine patterns of attack.

4.2.6.13. Conduct and manage Air Force vulnerability analysis and assistance functions in accordance with AFI 33-207, *Computer Security Assistance Program*. Notify COMAFFOR to JTF-GNO of technical vulnerabilities impacting Air Force computers and computer networks.

4.2.6.14. Assist the COMAFFOR to JTF-GNO in implementing the Air Force INFOCON program.

4.2.7. Coordinate with base NCC and theater NOSC to ensure presence of site personnel for troubleshooting operations when requested by JTF-GNO.

4.2.8. Participate in AFSN-led configuration control board to address AF-GIG requirements.

4.2.9. Provide situational awareness and status of the AF-GIG to SAF/XC, AFCA and to leaders at all levels based on their operational needs.

4.2.10. Assist COMAFFOR to JTF-GNO in building upon current Air Force policies and programs to implement and maintain a network security posture that will defeat hostile NetA and attempts to exploit the Air Force network.

4.2.11. Serve as the Air Force single point-of-contact for receiving reports from and reporting computer security incidents and vulnerabilities to organizations external to the Air Force.

4.3. Network Operations and Security Center (NOSC). The theater NOSC is the mid-level organization in the three-tiered NETOPS structure. A theater NOSC provides commanders with real-time operational network intrusion detection and perimeter defense capabilities, as well as theater-level NETOPS and fault resolution activities. This NETOPS entity is employed at the commander’s direction to defend information networks both in-theater and in-garrison. NOSC personnel monitor and support the day-to-day operational issues associated with their subordinate bases and units. Their mission focus is to ensure their theater’s operational and support systems are fully capable. As appropriate, they support their commanders with information assurance capabilities, such as information systems security, decision analysis, and other technological capabilities. Theater NOSCs will:

4.3.1. Operate 24-hours-a-day, 7-days-a-week.

4.3.2. Assist the AFNOSC (and DISA when requested through the AFNOSC) with ensuring presence of on-site personnel when requested by AFNOSC Net Operations Division to perform troubleshooting procedures to restore faulty, Air Force owned and operated, WAN transmission equipment and circuits.

4.3.3. Establish SLA, MOA, or MOU with Main Operating Bases (MOB), GSUs, tenant units, Air Force, and MAJCOM functional communities of interest defining agreed upon levels of support. Additionally, maintains SLA, MOA, or MOU with other NOSCs for providing back–up services as needed.

4.3.4. Perform Information Dissemination Management.

4.3.4.1. Implement, track, document, and report compliance with TCNOs directed by the AFNOSC. Issue NTOs, implement, track, document and report compliance with MAJCOM-level TCNOs. Ensure two-person compliance procedures are followed according to AFI 33-138 when implementing TCNOs. Issue and review all C4 NOTAMs for applicability to all theater unique information systems according to AFI 33-138.

4.3.4.2. Draft SITREPs according to AFI 10-206. Draft OPREP3s according to AFI 10-206 to document and report significant network events affecting theater-level systems.

4.3.4.3. Provide Help Desk services to NCCs and other NOSC customers for the theater; forward lessons learned and situations requiring additional assistance to next upper level tier Help Desk.

4.3.4.4. Provide situational awareness and visibility of the MAJCOM C4 systems as directed by the AFNOSC, but no less than every 12 hours, via NETCOP or other reporting methods as directed by the AFNOSC. As a minimum, NIPRNET, SIPRNET, Air Traffic Control and Landing Systems (ATCALS), Automated Security Incident Measurement (ASIM), weather systems, Automated Message Handling System (AMHS), Global Command and Control System (GCCS) and base level Telephony connectivity will be monitored. Other systems may be added as requirements dictate.

4.3.5. Perform System and Network Management.

4.3.5.1. Provide and manage external DNS service to assigned bases, and internal DNS service for IT services that are consolidated, and coordinate with AFNOSC Net Operations Division on Air Force-level DNS issues.

4.3.5.2. Manage theater-level (theater.af.mil, theater.ds.af.mil, theater.af.smil.mil, and theater.ds.af.smil.mil) DNS and assigned IP addresses. Those theater NOSCs that manage base-level IP addresses will follow guidance in paragraph **4.5.4.9.**

4.3.5.3. Perform distributed control of remote access services for the theater. Follow guidance in paragraph **4.5.4.9.2.1.**

4.3.5.4. Provide theater level Core Services (as defined in paragraph **6.4.**) to assigned bases.

4.3.5.5. Provide Network Time Protocol (NTP) management. NOSCs will use NTP on all systems within the CITS Network Management and Network Defense (NM/ND) boundary to synchronize system clocks with a local Global Positioning System (GPS) receiver. Additionally, ensure that as a minimum NTP is enabled on all core servers and backbone equipment.

4.3.5.6. Detect, respond, and report network events affecting operational availability of theater network, user service levels, support to critical applications, and core services to the AFNOSC and others as appropriate.

4.3.5.7. Provide technical assistance to assigned NCCs.

4.3.5.8. Perform system backup and disaster recovery procedures on NOSC managed core services.

4.3.5.9. Maintain capability to filter web sites to meet operational requirements, e.g., MINIMIZE.

4.3.5.9.1. Establish local procedures for notification of MINIMIZE according to Allied Communications Publication (ACP) 121/United States Supplement (US SUP)-1, (C) *Communication Instructions General* (U).

4.3.5.10. Monitor and manage Core Services via tools provided by the CITS Program Management Office.

4.3.6. Perform IA/NetD.

4.3.6.1. Provide support to the theater/Numbered Air Force (NAF) Information Warfare Flights.

4.3.6.2. Centrally operate and manage boundary protection and intrusion detection tools for all bases within their respective theater. This can be accomplished by either physically consolidating the servers at the NOSC or using remote management.

4.3.6.3. Protect against unauthorized intrusions and malicious activities; monitor and report intrusion detection activity according to AFI 33-138.

4.3.6.4. Monitor, detect, and implement NetD actions.

4.3.6.5. Maintain secure communications with AFNOSC Net Operations Division and NCCs.

4.3.6.6. Use vulnerability assessment software tools to analyze base networks under NOSC control for potential vulnerabilities and research/recommend appropriate protective measures. Report suspected vulnerabilities and recommended protective measures to the AFNOSC Net Security Division. Ensure vulnerability scans are run quarterly within their theater of responsibility.

4.3.6.7. Assists in developing a theater-level network security policy according to AFI 33-202,Volume 1.

4.3.6.7.1. Provide any network reports requested by the theater IA office required for Certification and Accreditation (C&A) of theater unique systems.

4.3.6.8. Analyze customer impact, within the theater, of all network incidents, problems and alerts, and develop corrective actions or management changes.

4.3.7. Take the following measures to meet the intent of the CSAF Server Consolidation effort:

4.3.7.1. Consolidate management of all theater external web servers (external web servers are those web servers that permit access to anyone from outside the .mil domain) to the NOSC. ANG shall consolidate to ROSC or NOSC locations where technically appropriate. Use remote management, co-location or shared hosting consolidation as best fits the operational mission.

4.3.7.2. Assist in consolidating all functional community of interest IT servers. Preferred location is to the DISA DECC, however, consolidation to the NOSC or ANG ROSCs is acceptable as well.

Consolidation could include using remote management, co-location, or shared hosting consolidation as best fits the operational mission. In some instances, consolidation to the NCC is more appropriate to the operational mission.

4.3.7.3. Manage desktop services (paragraph **6.4.4.**), consolidating services to the NOSC as best fits the operational mission.

4.3.7.4. Any new applications and their server(s), core services, network services, or desktop services and storage requirements shall meet the intent of the server consolidation architecture using remote management, co-location or shared hosting consolidation as appropriate to the operational mission in their initial operational capability and full operational capability.

4.3.8. Provide visibility of the theater network (NIPRNET and SIPRNET) to theater commanders and directors.

4.3.9. Provide NCCs, within the respective theater, visibility into NOSC-managed devices for local situational awareness.

4.3.10. Oversee implementation of policies, procedures, and special instructions to NCCs.

4.3.11. Support deployable operations and maintain joint capabilities.

4.3.12. Provide engineering guidance to plan, install, operate, and maintain base network hardware and software.

4.3.13. Perform NOSC-level systems control, maintenance, and administration functions within the theater network.

4.3.14. Manage theater electronic mail global address list.

4.3.15. Grant AFCA Scope EDGE personnel administrative access to NOSC and base networks to perform compliance assessments and optimization activities, as required by AFNOSC.

4.3.15.1. Scope EDGE personnel will complete local account access requirements prior to gaining local network access or provide proof of current IA training.

4.3.16. Perform Telephony Management and Voice Protection.

4.3.16.1. Provide centralized management and administration of the enterprise-wide Enterprise Telephony Management (ETM) platform.

4.3.16.2. Administer/disseminate Air Force and theater-wide voice protection system (VPS) policy (rule set) and site specific policies for each base and GSU in the enterprise.

4.3.16.3. Modify the active security policy (rule set) in the ETM platform as directed by higher headquarters to react to events, anomalies, and emergencies.

4.3.16.4. Maintain trained FSAs proficient in maintaining the server's operating system and ETM platform specific software.

4.3.16.5. Utilize platform to generate command-wide reports (as needed) and ensure real time visibility of voice networks.

4.3.16.6. Perform all management tasks for Fault, Configuration, Accounting, Performance, and Security (FCAPS).

4.3.16.6.1. Fault management tasks include but are not limited to detection, documentation and resolution of, application system faults, system detected telecommunication faults and supporting infrastructure faults.

4.3.16.6.2. Configuration management tasks include but are not limited to collection, configuration and identification of technical information of the VPS and the system's infrastructure, e.g., IPs and network IDs, firewall exceptions, Telco Trunk nomenclatures, telephone numbers and switching items, etc.

4.3.16.6.3. Accounting management tasks include but are not limited to control and maintenance of user accounts, system access passwords, telephony authorized control list (ACL) and firewall exceptions request.

4.3.16.6.4. Performance management tasks include but are not limited to control, manipulation, report generation and analysis of system collected data for base, theater and Air Force level management decision.

4.3.16.6.5. Security management tasks include but are not limited to detection, documentation, reporting and denial of access to unauthorized telephony exploitation.

4.3.17. Provide capability to automatically and continually capture, store, archive, and retrieve network topology and application traffic data for the purposes of all engineering functions listed in this document.

4.3.18. Achieve full operational capability within 4 hours after notification in situations requiring increased operations tempo surge manning. Annotate the 4-hour response time in section IIB of AF IMT 723, **Sorts Doc Statement**, and state AFI 33-115, Volume 1, as the response time source reference document. Does not apply to AFRC and ANG.

4.3.19. Will, along with the NCC and CSAs, be responsible for public key infrastructure (PKI) enable devices on the network. Complete PKI responsibilities can be located in AFMAN 33-223, *Identification and Authentication.*

4.3.20. Partner with the MAJCOM/base records manager to ensure records management procedures are implemented and sustained for all enterprise storage services.

4.4. Integrated Network Operations and Security Center (I-NOSC).

4.4.1. I-NOSC is the next evolution of our Air Force networks. They will:

4.4.1.1. Perform work done at present MAJCOM NOSCs under the command of the AFNETOPS/CC. These regional I-NOSCs give commanders visibility into the network to achieve operational objectives. I-NOSCs must establish the ability to provide commanders a real time presentation of their network forces. Within their theater, each I-NOSC manages functions currently performed by MAJCOM NOSC i.e., network defense; generates an enterprise situational awareness picture; manages network configuration; and provides information assurance and Spectrum management. This includes voice, video, and data networks supported by the GIG. I-NOSCs must quickly evolve toward full operational capability to remotely administer base-level file, print, and messaging servers, followed by remote management of applications servers within their AOR.

4.4.2. Implementation.

4.4.3. The Integrated NOSC is the Air Force's operational-level warfighting command center for network defense and network transport. The I-NOSC is the execution arm of the AFNOSC and provides command and control, and defense of the Air Force-provisioned portion of the GIG (Constellation-Net).

4.4.4. The I-NOSC ensures Air Force networks are capable of conducting, supporting, and advancing coalition, joint, Air Force, and interagency operations. Through a common environment, the I-NOSC provides situational awareness to the AFNOSC, WFHQ, and MAJCOMs. Each I-NOSC will oversee the operation of the base level NCCs, while providing remote administration of enterprise-wide infrastructure.

4.4.5. Implementation Strategy.

4.4.5.1. The implementation plan (I-Plan) takes into consideration the equipment and technical aspects needed to satisfy I-NOSC final operating capability (FOC) for terrestrial networks. The I-Plan discusses personnel and the requirements to support the I-NOSCs without developing a plan for the personnel moves.

4.4.5.2. Airborne and Space networks will be migrated by FY10; however, this plan will not outline their full implementation into the I-NOSC.

4.4.5.3. Initial operating capability (IOC) occurs when an I-NOSC has operational control over any part of the Air Force-provisioned portion of the GIG not currently under the Network Operations Division (NOD) and National Security Directorate (NSD) control. FOC occurs when the entire terrestrial portion of the Air Force-provisioned portion of the GIG is under direct command and control of an I-NOSC.

4.4.5.4. The strategy is divided into spirals that take command and control of the network in a top-down approach. Spirals are implemented across an I-NOSC's area of responsibility (AOR). The spirals drill down to assume control of the enterprise network one layer at a time. This strategy is in contrast to a MAJCOM-by-MAJCOM or base-by-base strategy which would assume control of a MAJCOM or base in its entirety before assuming control of the next MAJCOM or base.

4.4.5.5. The AF-GIG architecture must mature incrementally to migrate to the desired end-state. This incremental change correlates to a phased approach to establish or realign AF-GIG operations conducted across the three network operations tiers, i.e., the AFNOSC, I-NOSCs, and NCCs. The first phase is near term and prescribes an architecture that will be in place by FY06. The final phase identifies the end state architecture which is targeted for FY11.

4.5. Network Control Center (NCC) The NCC oversees network operations, helps achieve information assurance, and generates visibility into the base network. Wing and theater air base commanders exercise command and control over their fixed base or deployed site networks and systems via the NCC. Local Area Networks (LAN) and the Metropolitan Area Networks (MAN) on the base are considered part of the base network and managed by the NCC. Thus, the NCC is the central focal point on base for the operation, maintenance, and management of all aspects of the base network to include wireless LANs (NCCs will need to establish a memorandum of agreement with the appropriate functional community to cover manning and training deficiencies that may exist due to legacy wireless equipment). The NCC provides an on-site technical capability to implement physical network changes and modifications and restoration of faulty network transmission equipment and circuits when directed by the NOSC or AFNOSC. Using network administration, network management, and information protection tools, the NCC technicians provide core services to FSAs, CSAs, and users. The NCC is also responsible for all PKI enabled devices located under their area of responsibility. Complete PKI responsibilities can be located in AFI 33-202, Volume 6, *Identity Management*. NCCs will:

4.5.1. Operate 24-hours-per-day, 7-days-per-week (with either continuous manning or on-call after-hours response capability). ANG and AFRC operates on 40-hour work week (Monday-Friday).

4.5.2. Ensure presence of on-site personnel when directed by NOSC or AFNOSC .

4.5.3. Achieve full operational capability within 4 hours after notification in situations requiring increased operations tempo surge manning. This ensures on-site presence of personnel to meet elevated unit communications requirements. Units will annotate the 4-hour response time in section IIB of AF IMT 723 and state AFI 33-115, Volume 1, as the response time source reference document. Does not apply to AFRC and ANG.

4.5.4. Perform Information Dissemination Management.

4.5.4.1. Implement NETOPS tasking order (NTO) as required. Implement TCNOs according to AFI 33-138. Ensure two-person compliance procedures are followed according to AFI 33-138 when implementing TCNOs. Utilize C4 NOTAMs according to AFI 33-138.

4.5.4.2. Draft SITREPs according to AFI 10-206. Draft OPREP3s according to AFI 10-206 to document and report significant network events affecting base-level systems.

4.5.4.3. Provide Help Desk services to base-level users and CSAs to serve as focal points for network, to include Air Force IT services, problem resolution. Forward lessons learned and situations requiring additional assistance to next upper level tier Help Desk.

4.5.4.4. Escalate problems beyond the capability of the NCC to the NOSC for resolution and info the theater IA office if required.

4.5.4.5. Provide situational awareness and visibility of the base-level C4 systems as directed by the NOSC, but no less than every 12 hours via NETCOP. As a minimum, NIPRNET, SIPRNET, Defense Switched Network (DSN), ATCALS, ASIM, weather systems, AMHS, and GCCS will be monitored. Other systems may be added as requirements dictate. Forward requirements to HQ AFCA/ECN. (Does not apply to ANG NCC. ANG Regional Operations Security Center (ROSC) performs this function.)

4.5.4.6. Provide flexible and scalable levels of service to FSAs, CSAs, and users for Air Force IT services as defined by the SAF/XC.

4.5.4.7. Perform System and Network Management.

4.5.4.8. Manage internal base DNS if not centrally managed by the theater NOSC.

4.5.4.9. Manage all base IP address space through utilization of Dynamic Host Configuration Protocol (DHCP). DHCP will allocate dynamic IP addresses for:

4.5.4.9.1. All noncritical workstations connected to the internal base network. Noncritical workstations will have a lease of 30 days applied to them; this ensures, with relative certainty, that the same IP is assigned to a workstation each time a new reservation is issued. In instances where there is a documented IP address shortage for a DHCP scope (e.g., more than 80 % utilization), the lease time can be adjusted to a shorter lease duration for that particular scope so that IP addresses can be recovered more quickly. Does not apply to the ANG.

4.5.4.9.2. Remote Access Clients. The use of a remote access modem will be accomplished according to AFI 33-202, Volume 1.

4.5.4.9.2.1. In coordination with the NOSC, provide and control all remote dial-in/dial-out communications access services. Place the communications server capable of handling dial-in and dial-out services within the CITS network battle management/network defense (NBM/ND) boundary to prevent the possibility of back-door access. This means that organizations will not connect external access devices to the base network. The NCC controls all remote dial-in/dial-out communications services. The NCC will place all remote dial-in/dial-out communications servers (remote access servers) on an alternate interface (not the internal or external interface) of the firewall. If an alternate interface is not available the remote access server will be placed off the external interface of the firewall. (Does not apply to ANG NCC.)

4.5.4.9.2.2. ANG NCC. CITS does not provide ANG NCCs with NBM/ND equipment. ANG purchases firewalls (CITS supported) for each NCC. The NCC controls all remote dial-in/dial-out communications services. The NCC will place all remote dial-in/dial-out communications servers (remote access servers) on an alternate interface (not the internal or external interface) or the firewall.

4.5.4.9.2.3. The ANG NCC will use NTP on all systems within the security boundary to synchronize system clocks with a local GPS receiver or approved DOD source. Additionally, ensure that as a minimum NTP is enabled on all core servers and backbone equipment capable of using NTP. Preferably do not allow external NTP sources through the NBM/ND boundary due to inherent security problems. However, ANG NCCs that receive NTP from their upper level ROSC may permit NTP through the firewall by exception only (e.g., IP address to IP address).

4.5.4.9.2.4. Provide NTP management. NCCs will use NTP on all systems within the CITS NBM/ND boundary to synchronize system clocks according to NCC technical order (TO). Additionally, ensure that as a minimum NTP is enabled on all core servers and backbone equipment capable of using NTP. Do not allow external NTP sources through the NBM/ND boundary due to inherent security problems. (Does not apply to ANG NCC.)

4.5.4.10. Move all Air Force owned networks behind the NCC/NOSC/ANG ROSC IA boundary. NOSC, ANG ROSC, or NCC will manage and monitor all networked devices using network management and security tools. In all cases, host tenant agreements and service level agreements that result from this requirement must adhere to Air Force policy. The following scenarios apply to non-Air Force units residing on an Air Force base:

4.5.4.10.1. All non-Air Force units on an Air Force installation that use the host base's Core Services (see **Chapter 6**) must be located behind the security boundary and comply with the security policy for the host base network.

4.5.4.10.2. Report all backdoors within 24 hours of discovery to NOSC. Inform NOSC on backdoor remediation progress.

4.5.4.10.3. Any non-Air Force unit on an Air Force installation not using host base Core Services (see **Chapter 6**) may have their own network separate from the base network. These networks must adhere to the following guidelines:

4.5.4.10.3.1. Physically separate this network from the base network infrastructure. No devices on this network may attach to the base data network in any way.

4.5.4.10.3.2. This network must connect outside the security boundary and may only communicate with the base network by coming through the security boundary from the outside. ANG sites will connect external site (non GSU) connections to dedicated firewall interface to maintain appropriate security posture.

4.5.4.10.3.3. The using organization is responsible for funding any and all network components as well as any costs associated with their connectivity.

4.5.4.10.3.4. The using organization is responsible for complying with all DOD-required IA measures, to include intrusion detection and vulnerability patching.

4.5.4.10.3.5. Provide messaging services to base-level users [e.g., AMHS and Simple Mail Transfer Protocol (SMTP) electronic mail]. NCCs are not required to do this if the NOSC is performing these duties.

4.5.4.10.4. All Air Force military and civilian members will be issued an E-mail address. This is a mandatory compliance issue.

4.5.4.10.5. All Air Force members in a non-Air Force unit residing on an Air Force base will have an Air Force E-mail account supported by the local base NCC or supporting NOSC .

4.5.4.10.5.1. All Air Force members on DOD sites will have an Air Force E-mail account from the Air Force base NCC or supporting NOSC which supports the members servicing Military Personnel Flight (MPF). If the unit does not have an Air Force servicing MPF, then the next paragraph applies.

4.5.4.10.5.2. All Air Force members assigned to any non-DOD site will have an "af.mil" E-mail account established through the 11th Communications Squadron. Members will have access via web mail.

4.5.4.10.5.3. All new accessions will have an Air Force E-mail account established upon completion of basic training or their commissioning source. This will either be at tech school or their first assignment, which ever occurs first.

4.5.4.10.5.4. E-mail accounts will remain active and available for 60 days following a member's permanent change of station (PCS). After 60 days the contents of the users email account will be transitioned by the loosing NCC or supporting NOSC to the newly created email account at the gaining base. After this transition, the old email account will be deleted and the gaining base NCC will notify the base MPF of the members new email address for loading into MILPDS. This is a requirement by AF/DP due to the closing of some base level MPF functions – no airman can be without an email account at any time, due to it being used by AFPC for personnel matters.

4.5.4.10.5.5. The E-mail account and all associated E-mail for members separating will be deleted 60 days after departure. Departing members can access the account via web mail.

4.5.4.10.6. Secure and manage the CITS Common Air Force Wireless solution.

4.5.4.10.6.1. NCCs will control any hardware or software used to provide wireless access to the base network.

4.5.4.10.6.2. All client devices using the base wireless infrastructure will meet the requirements specified in AFI 33-202, Volume 1, and the CITS common Wireless Local Area Network (WLAN) solution or have an approved waiver on file. In addition:

4.5.4.10.6.3. Wireless client devices must be registered with the NCC prior to connecting to the base wireless infrastructure. At the time of registration, the NCC will record a device specific authentication factor--usually the Media Access Control (MAC) address of the device--to be used for hardware authentication.

4.5.4.10.6.4. Lost or stolen wireless devices must be reported to the NCC as soon as possible. Entries for such devices will be removed from all access control lists. If recovered, the device-specific authentication factor will be considered compromised and will be changed before the device is redeployed.

4.5.4.10.6.5. All wireless client devices must run approved Air Force-approved antivirus software.

4.5.4.10.6.6. All wireless client devices must use a Federal Information Processing Standard (FIPS) certified secure client (usually software) compatible with the wireless local area network gateway/switch managed by the NCC.

4.5.4.10.6.7. Wireless client devices will not allow ad hoc wireless networking or direct peer-to-peer wireless networking.

4.5.4.10.6.8. Systems with direct network access (e.g., via Ethernet) will not provide wireless data connectivity. Any network device with an external wireless network interface or an integrated wireless interface must have the wireless interface disabled prior to connecting to the wired network via fiber or Ethernet. The method for disabling the integrated interface will be through the use of an automated software solution that enforces required security policies. Devices that have integrated wireless Network Interface Cards (NIC) which cannot be disabled via an automated process, require theater designated approving authority (DAA) approval prior to manually disabling the wireless NIC and connecting to the wired network. Due to their low risk, wireless pointing devices are not required to use encryption.

4.5.4.10.6.9. Passwords and sensitive information will not be wireless transmitted unless encrypted in accordance with Air Force WLAN policy outlined in AFI 33-202, Volume 1, and AFMAN 33-223. This includes wireless keyboards and wireless terminals, but not pointing devices.

4.5.4.11. Network Operations Requirements.

4.5.4.11.1. Except for the ANG, must integrate into CITS and NBM/ND suite at NOSC and/or NCC.

4.5.4.11.2. Must have the capability to shut down wireless access points remotely from the NCC and NOSC.

4.5.4.11.3. NCCs will expand current network vulnerability scanning procedures to include wireless networks.

4.5.4.11.4. Provide a core set of office automation application support services.

4.5.4.11.5. Implement software patches and security fixes as required by the NOSC, AFNOSC, or program manager.

4.5.4.11.6. Report events not previously detected by the NOSC or AFNOSC.

4.5.4.11.7. In coordination with NOSC, plan, install, operate, and maintain base network hardware and software.

4.5.4.11.8. Perform regular day-to-day system backup and recovery operations on NCC managed servers. At a minimum of once a quarter, test recovery procedures to ensure procedures are accurate and operational.

4.5.4.11.9. Develop local restoral and contingency operations plans from existing operations/war plans. Validate restoral plans by testing them on at least a biannual basis.

4.5.4.11.10. Maintain network and facility configuration, migration, and upgrade plans.

4.5.4.11.11. Perform fault management for the local base network.

4.5.4.11.11.1. Dispatch technicians to unmanned or user and subscriber locations when required to test, troubleshoot, and restore service.

4.5.4.11.11.2. Coordinate with job control subscribers, local and distant support agencies, and contractors to isolate faults, restore service, and make repairs.

4.5.4.11.11.3. Ensure a trouble-call process is established.

4.5.4.11.12. Provide network and small computer maintenance support to CSAs and FSAs.

4.5.4.11.13. Provide technical support to FSAs and CSAs when requested and maintain an electrostatic discharge maintenance area. See TO 00-25-234, Chapter 7, for guidance.

4.5.4.11.14. Perform fault isolation to the line replaceable unit (LRU) and line item equipment level. Fault isolation methods include automated diagnostics and sound troubleshooting techniques.

4.5.4.11.15. Perform configuration management for the local base network. Work with the functional on base for implementation of systems. Provide a database of ports, protocol and services that are associated with a particular system. ANG uses central DB and NOSC.

4.5.4.11.16. Prepare and update network maps and facility equipment listings. Provide theater NOSC a copy as required.

4.5.4.11.17. Establish a maintenance contract and warranty plan according to **Chapter 10**.

4.5.4.11.18. Establish a license management program according to AFI 33-114, *Software Management*, to ensure authorized usage for base network software.

4.5.4.11.19. Work with Planning/Implementation section and the Systems Telecommunications Engineering Manager (STEM) to participate in the review and planning of base transmission media and telecommunications systems networks. Makes sure replacements for legacy or dumb network devices incorporate remote management capability to improve centralized management, performance, and quality.

4.5.4.11.20. Perform minor application enhancement and software metering according to AFI 33-114.

4.5.4.11.21. Perform information technology (IT) equipment custodian (EC) duty for NCC equipment as directed by AFI 33-112, *Computer Systems Management* (will become Information Technology Asset Management [ITAM]).

4.5.4.11.22. Provide assistance, when needed, and perform cryptographic equipment updates on devices under the control of the NCC.

4.5.4.11.23. Provide base network/NCC hardware and software installation service.

4.5.4.11.23.1. Hardware: NCCs install and configure network servers, routers, hubs, bridges, repeaters, and servers. They test and document equipment installation acceptance testing. The ANG shall follow NOSC direction for centrally managed enterprise systems (AD, Exchange, etc).

4.5.4.11.23.2. Software: NCCs receive and inventory network software according to AFI 33-114, test and validate new software applications and network operating systems.

4.5.4.11.23.2.1. Distribute and install network software releases and updates, and assist customers with software installation and customization.

4.5.4.11.23.2.2. Install and configure SMTP hosts, relays, and gateways. The ANG shall follow NOSC direction for configuration.

4.5.4.11.23.2.3. Review site license agreements and remove software from systems when no longer required or authorized. Dispose or redistribute excess software according to AFI 33-114.

4.5.4.11.24. Perform base NM planning.

4.5.4.11.25. Maintain the base network characterization and validate the DISA Minimum Essential Circuit Listing (MECL) and the Defense Information Technology Contracting Office (DITCO) database product.

4.5.4.11.25.1. Collate local and long-haul customer telecommunications circuit information.

4.5.4.11.25.2. Verify current network configurations against other agency databases and forward corrections as required. (May be performed in your circuit actions office.)

4.5.4.11.26. Perform base-wide configuration standardization and interface engineering.

4.5.4.11.26.1. Prepare and update in-station system block diagrams, network maps, and facility equipment listings; maintain network and facility configuration plans; perform minor network engineering; monitor management information base variables; and advise and make recommendations on new systems to customers.

4.5.4.11.27. Perform the following in conjunction with the base Communications and Information Systems Officer and plans function:

4.5.4.11.27.1. Review Project Support Agreements (PSA) and coordinate corrections with the appropriate agencies.

4.5.4.11.27.2. Coordinate with Engineering and Installation (EI) teams and/or commercial vendors prior to arrival and prepare the facility for installation team.

4.5.4.11.27.3. Escort and assist team chiefs with installation or upgrade projects.

4.5.4.11.27.4. Complete DD Form 250, **Material Inspection and Receiving Report**; AF IMT 1261, **Communications and Information Systems Acceptance Certificate;** and EI critiques.

4.5.4.11.28. Perform contract management for base network support.

4.5.4.11.28.1. Consolidate and evaluate base-wide NCC-managed network and system components as candidates for contract maintenance support.

4.5.4.11.28.2. Submit inputs to the unit plans function for statement of work development.

4.5.4.11.28.3. Assist the plans function in the preparation of quality assurance surveillance plans and perform contract quality assurance evaluation functions as identified.

4.5.4.11.29. Perform base network budget planning.

4.5.4.11.29.1. Develop/submit budget input and request higher-level funding for all NCC requirements and operations functions.

4.5.4.11.29.2. Monitor base network funds availability and process Government Purchase Card (GPC) requests for hardware and software purchases according to AFI 64-117, *Air Force Government-Wide Purchase Card (GPC) Program*.

4.5.4.11.30. Remotely perform the functions and duties of a Defense Communications System (DCS) Primary Systems Control Facility (PSCF), patch and test facility, DCS switching center, or other DCS operations function, when it is technically and economically feasible and does not degrade quality of service in accordance with DISA procedures. To support the wing during contingencies, the NCC takes over the responsibility and authority of the PSCF for DCS service control.

4.5.4.11.31. Conduct performance management for the local base network.

4.5.4.11.32. Consolidate base-level network performance data, security data, and analysis reports, pulling information from the Air Force NETOPS hierarchy as needed. Use the consolidated information to identify causes of service, performance, and security flaws. On the basis of the aggregated analysis, recommend changes in network configurations, hardware or software, procedures, and staff training.

4.5.4.11.33. Monitor and optimize network performance.

4.5.4.11.34. Coordinate installation, acceptance testing, quality assurance, fault isolation, and restoration of the infrastructure with the base's other communications unit functions.

4.5.4.11.35. Maintain capability to filter web sites to meet operational requirements (e.g., MINIMIZE). NCCs are not required to do this if the NOSC or ANG ROSC is performing these duties.

4.5.4.11.36. Establish individual circuit and system parameters on non-DCS circuits. Develop the parameters according to DISAC 300-175-9, *DCS Operating Maintenance Electrical Performance Standards*, supplemented by commercial-leased equipment and circuit performance standards.

4.5.4.11.37. Establish initial performance thresholds according to systems and circuit operation specifications and operational or mission requirements.

4.5.4.11.38. Remotely test subscriber equipment, end-to-end circuits, systems, and networks to verify the services provided and input and output signals meet standards.

4.5.4.11.39. Adjust remote network element equipment to optimize service.

4.5.4.11.40. Record configuration data, test data, failure symptoms, coordination efforts, fault isolation steps performed, and any other useful information. Use this information to evaluate and control operations, service capabilities, and service quality.

4.5.4.11.41. Report to management on quality of infrastructure services.

4.5.4.11.41.1. Perform system diagnostics and set global alarm thresholds and system parameters.

4.5.4.11.41.2. Utilize performance tools to ensure optimum network operation, monitor system logs, analyze bandwidth utilization, and set global parameters to prevent adverse effects to the overall communications network. Core systems must have critical path redundancy.

4.5.4.11.42. Perform network/circuit Quality Control (QC) testing and evaluation.

4.5.4.11.42.1. Generate and update QC schedules.

4.5.4.11.42.2. Plan, provide, coordinate, and verify alternate service during QC testing.

4.5.4.11.42.3. Access and monitor Preventative Maintenance Inspection (PMI) schedules published by the maintenance control work center.

4.5.4.11.42.4. Coordinate in-service/out-of-service QC testing and performance of PMIs with affected work centers and external agencies.

4.5.4.11.42.5. Coordinate and deactivate alternate service once testing/PMIs are completed and original circuit/equipment is verified operational.

4.5.4.11.42.6. Analyze QC performance trend analysis data (collected through in-service/out-of-service QC testing) to identify trends or patterns of circuit/system/network degradation, dispatch to and from user locations when required, and generate and analyze outage reports.

4.5.4.11.42.7. Submit DD Form 1368, **Modified Use of Leased Communication Facilities**, when required, and research, prepare, and submit QC waiver requests when necessary, in the absence of a systems control facility.

4.5.4.11.43. Conduct security management for the local base network.

4.5.4.11.43.1. Conduct Information Protection Operations (IPO) according to applicable security publications and TTPs.

4.5.4.11.44. Install and set up audit tools.

4.5.4.11.45. Perform IA/NetD.

4.5.4.11.45.1. Perform vulnerability assessments to test and validate security of networks and systems. If vulnerabilities are discovered, provide appropriate systems administrators, unit commanders, DAA, wing and theater IA offices, and AFNOSC with test results and recommendations. Report vulnerabilities found according to AFI 33-138.

4.5.4.11.45.2. Conduct daily traffic analysis, identify and characterize incidents, and generate incident reports with Air Force approved intrusion detection tools. Investigate each item to clarify and resolve suspicious activity. Report validated suspicious activity according to AFI 33-138. The NCC does not need to perform this function if it is done at the theater NOSC. (Does not apply to ANG NCC. ANG ROSC performs this function.)

4.5.4.11.45.3. Review AFNOSC advisories and verify systems under NCC control are protected against documented vulnerabilities.

4.5.4.11.45.4. Notify information systems security officers (ISSO), CSAs, FSAs, and/or users when their computers have weak configurations, vulnerabilities, and when they have been accessed, exploited, or destroyed by unauthorized persons or machines.

4.5.4.11.45.5. Put users of Air Force computer systems, including computers connected to a network, stand-alone computers, and portable (wireless) computers, on notice that their use constitutes consent to monitoring as specified in AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP).*

4.5.4.11.45.6. Get AF-GIG DAA (8 AF/CC) approval before connecting to the base network infrastructure. Terminate service and/or network connectivity of local systems and networks that fail to comply. Does not apply to the ANG.

4.5.4.11.45.7. Provide, manage, and control (in coordination with the AFNOSC when required) access to NIPRNET, SIPRNET, and the Internet.

4.5.4.11.45.8. The NCC, in coordination with the NOSC, will manage any/all security policy enforcement tools and monitor all networked devices.

4.5.4.11.45.9. Equip all servers within the CITS NBM/ND boundary with host-based intrusion detection and network security analysis and scanning tools. Does not apply to ANG/NCCs.

4.5.4.11.45.10. Identify weak configurations and security holes by auditing and monitoring events occurring on the network.

4.5.4.11.45.11. Monitor audit and error logs for security violations.

4.5.4.11.45.12. Test and validate network security to establish and maintain a target baseline for Air Force owned systems.

4.5.4.11.45.13. Identify and secure computer systems on an affected network. Identify computers with exploited vulnerabilities.

4.5.4.11.45.14. Provide any network reports requested by the wing IA office required for C&A of base networks and systems.

4.5.4.11.45.15. Assists in developing a base-wide network security policy according to AFI 33-202, Volume 1.

4.5.4.11.45.16. Coordinate on all base unique C&A packages or requests.

4.5.4.11.45.17. Develop local procedures to report and respond to computer security and virus incidents according to AFI 33-138. Work with the wing IA office to identify internal actions such as local reporting channels, criteria for determining who is notified, etc.

4.5.4.11.45.18. Perform local NetD actions and respond to NOSC or AFNOSC direction.

4.5.4.11.45.19. Ensure physical security of all local AF-GIG infrastructure components regardless of their locations.

4.5.4.11.45.20. Analyze customer impact, within the base, of all network incidents, problems and alerts, and develop corrective actions or management changes.

4.5.4.11.45.21. In coordination with the theater NOSC, take the following measures to meet the intent of the CSAF Server Consolidation effort:

4.5.4.11.45.21.1. Consolidate all E-mail, file, internal (inside the firewall) web and print servers to the theater NOSC, ANG ROSC, or NCC, using remote management, co-location or shared hosting consolidation as best fits the operational mission.

4.5.4.11.45.21.2. Consolidate functional community of interest to the NCC if they cannot be consolidated at the DECC or NOSC using remote management, co-location or shared hosting consolidation as best fits the operational mission.

4.5.4.11.45.21.3. Perform remote management of desktop services (paragraph **6.4.4.**), consolidating services to the NCC as best fits the operational mission.

4.5.4.11.45.21.4. Familiarize and guide FSAs and CSAs on local network operations and procedures.

4.5.4.11.45.21.5. Establish, maintain, control, and enforce the base Internet use policy according to AFI 33-129, *Web Management and Internet Use.*

4.5.4.11.45.21.6. Grant AFCA Scope EDGE personnel administrative access to base networks to perform compliance assessments and optimization activities, as requested by their parent MAJCOM.

4.5.4.11.45.21.7. Partner with the base records manager to ensure records management procedures are implemented and sustained for all enterprise storage services.

4.6. Functional Systems Administrator (FSA). FSAs ensure functional communities of interest systems, servers, workstations, peripherals, communications devices, and software are on-line and supported. They must thoroughly understand the customer's mission and be completely knowledgeable of hardware and software capabilities and limitations supporting that functional system. Their responsibilities extend from the user's terminal to the server, but do not normally include the network backbone infrastructure unless established by separate SLA, MOA, or MOU or as directed by AFFOR A-6 in deployed environments. FSAs are not normally assigned to the NCC, but are a logical extension of NCC functionality. FSAs may have Air Force specialty codes (AFSC) from various functional communities (i.e., supply, personnel, maintenance, etc.) FSAs function at the IT-2 (DOD 8500.2) and ADP-2 (DOD 5200.2-R) level. FSAs will:

4.6.1. Comply with the policies of this instruction. Perform the responsibilities delegated by the NCC to optimize performance and quality of service. Consolidate systems administration duties within an organization or a building, if possible, merging them with the NCC based on an SLA, MOA, or MOU.

4.6.2. Ensure servers, workstations, peripherals, communications devices, and operating system/ application software are properly configured for network operation, are on-line, and are available to customers.

4.6.3. Periodically review the organization's needs for computer resources.

4.6.4. Define ownership of applications and determine who has permission to read, write, and execute.

4.6.5. Assign and maintain user IDs and passwords according to AFMAN 33-223. Administer user privileges on the system (e.g., when users share files).

4.6.6. Plan for short-term and long-term loss of system hardware and software. In configuring the system, the FSA and network security manager must decide on contingency plans in case of the FSA’s absence. This may involve having another FSA administer the system remotely.

4.6.7. Monitor the efficiency of the system (e.g., finding and resolving system bottlenecks).

4.6.8. Perform routine system maintenance such as backing up or archiving application data files and adding application software updates.

4.6.9. Serve as the system troubleshooter, a critical role in keeping the system operational. Contact the NCC for hardware maintenance when necessary.

4.6.10. Work with the NCC to implement network security policies and procedures as outlined in the base network security policy.

4.6.11. Ensure end user training is conducted.

4.6.12. Provide user manuals that include sign-on and sign-off procedures, use of basic commands, software policies, user responsibilities, etc.

4.6.13. Implement software patches and security fixes as required by the AFNOSC or program management office. Test and validate the proper operation and configuration with appropriate patches and fixes, as required above, prior to restoring any device to the network.

4.6.14. Ensure physical security of unit AF-GIG components.

4.6.15. Monitor difficulty reports, heads-up messages, and system advisory notices.

4.6.16. Prior to gaining MAJCOM installation of network equipment on ANG sites, ANG/SC approval is required.

4.7. Client Support Administrator (CSA). CSAs serve as the first line of help to resolve customers’ administrative and technical problems. CSAs are usually not assigned to the NCC, though are logically an extension of the Help Desk team. CSAs take direction from the NCC and FSA. NCC direction takes precedence over FSA direction. CSAs install, configure, and operate client/server devices. The CSA will be a 3A0X1 unless none are assigned. When a 3A0X1 is not assigned, any AFSC or occupational series can perform CSA duties once trained and certified. Foreign nationals can be assigned CSA duties if trained and certified. CSAs will:

4.7.1. Comply with the policies of this instruction and AFI 33-115, Volume 2.

4.7.2. Perform the installation of equipment, connection of peripherals, and the installing/deleting of client level software. Ensure physical security of unit AF-GIG components.

4.7.3. Configure client level software, modify software configuration, and perform basic configuration management functions.

4.7.4. Provide software application assistance for commonly used office automation applications purchased from standard Air Force support contracts. Include support to standard wireless office automation devices.

4.7.5. Perform initial client workstation diagnostics and troubleshooting of client workstations assigned to them.

4.7.6. Assign, modify, and delete passwords and user privileges according to AFMAN 33-223.

4.7.7. Report security breaches and distribute security information according to AFI 33-138 and local policies.

4.7.8. Coordinate support issues with all agencies (e.g., customers, FSA, NCC, etc.).

4.7.9. Notify the unit EC of any hardware relocation and equipment problems.

4.7.10. Obtain an implementation checklist from the theater NOSC, NCC, or FSA, before installing any equipment. Assist with installing, testing, and accepting new systems according to the terms of the purchase contract and instructions.

4.7.11. Coordinate with the facility manager and the base civil engineer for facility support requirements.

4.7.12. Periodically review the organization's needs for computer resources.

4.7.13. Validate computer equipment requirements the unit EC submits.

4.7.14. When requested, assist the unit EC with computer hardware and software inventories.

4.7.15. Promote user awareness concerning unauthorized or illegal use of computer hardware and software.

4.7.16. Identify organization deficiencies and operational needs that computer use can solve.

4.7.17. Ensure organizations do not use shareware or public domain software until approved for use by the DAA after the ISSO, CSA or FSA ensures it is free of viruses, hidden defects, and obvious copyright infringements.

4.7.18. Assist unit with client workstation (C&A) process.

4.7.19. Implement client workstation software patches, security fixes, and service releases according to local NCC instructions.

4.7.20. Perform E-mail management, when technically feasible.

4.7.20.1. Create/Configure mailboxes (user, custom).

4.7.20.2. Create Public/Personal/Private folders.

4.7.20.3. Move mailboxes.

4.7.20.4. Perform mail box maintenance.

4.7.20.5. Create Distribution lists.

4.7.20.6. Track messages (concepts – read receipts).

4.7.20.7. Perform Directory Service support; ability to create directories on shared drives and assign/grant permissions.

Chapter 5

AIR FORCE GLOBAL INFORMATION GRID (AF-GIG) ACTIVE DIRECTORY MANAGEMENT

5.1. Overview.

5.1.1. Standardization of naming conventions for Active Directory objects and attributes are critical for interoperability and configuration control reasons.

5.2. Authority.

5.2.1. Per SAF/XCI guidance, "Rigorous central control will be exercised over Active Directory naming conventions." HQ AFCA/ECSO is the lead for all Active Directory concerns to include the responsibility for establishing naming conventions. Theater NOSCs and base-level NCCs are responsible for enforcement of naming conventions. AF-GIG naming convention guidance can be found in AFI 33-119, *Air Force Messaging*. Additional information or questions should be referred to **afca.ecso@scott.af.mil**.

5.2.2. The Air Force will have multiple forests consisting of a single forest per MAJCOM. This requirement holds true for both NIPRNET and SIPRNET. Additional roots will not be considered.

5.2.3. HQ AFCA/ECSO is the Air Force focal point for Active Directory requirements, standardization and processing. In all cases, HQ AFCA/ECSO will be formally notified of all Active Directory planning and implementation. MAJCOMs will send a copy of their Active Directory implementation to HQ AFCA/ECSO.

Chapter 6

MISSION AREAS, NOSC OPERATIONS, CREW POSITIONS AND CORE SERVICES

6.1. Mission Areas. AFNETOPS Mission Areas are the overarching activities performed by assigned CSAs to maintain and operate the AF-GIG and enable Air Force operations. These actions promote information assurance and enable crew members to maximize operational availability, optimize performance, and mitigate risks.

6.1.1. Systems and Network Management (S&NM).

6.1.1.1. The S&NM mission area includes the range of computing hosts and applications connected by transmission systems, both wired and wireless, that carry voice, data, sensor, and video throughout the AF-GIG. It includes switched, fiber channel, routed, video teleconferencing (VTC), satellite communications, and wireless networks. S&NM comprises the functions of FCAPS management.

6.1.1.2. This mission area is focused on Assured Resource (System and Network) Availability and on Assured Information Delivery. The objectives of this focus are achieved by configuring and allocating AF-GIG system and network resources; ensuring effective and efficient processing, connectivity, routing, and information flow; accounting for resource usage; and maintaining robust AF-GIG capabilities in the face of component or system failure and/or adversarial attack.

6.1.2. Information Dissemination Management (IDM).

6.1.2.1. The IDM mission area provides the right information to the right person in the right format at the right place and time in accordance with commander's information dissemination policies while optimizing the use of information infrastructure resources. IDM, a subset of information management, provides services that address awareness, access, and delivery of information. It involves the operations of compiling, cataloguing, caching, distributing, and retrieving data. It also manages the information flow to users and enables execution of the commander’s information policy IDM relies on information awareness, information access, delivery management, and dissemination support.

6.1.2.2. This mission area is focused on Assured Information Protection and Assured Information Delivery whose objectives are achieved through the efficient movement of information into, within, and out of the AF-GIG, the secure storage of information, and the capacity to rapidly compile and catalogue new collections of information for availability to prospective users. Decisions regarding availability must be guided by warfighter needs, access commensurate with information security requirements, and the most efficient and effective modes of information delivery and retrieval.

6.1.3. Information Assurance/Network Defense (IA/NetD).

6.1.3.1. The IA/NetD mission area helps ensure the availability, integrity, identification, authentication, confidentiality, and nonrepudiation of friendly information and information systems while denying the adversaries access to the same information/information systems. It also provides end-to-end protection to ensure data quality and protection against unauthorized access and inadvertent damage or modification.

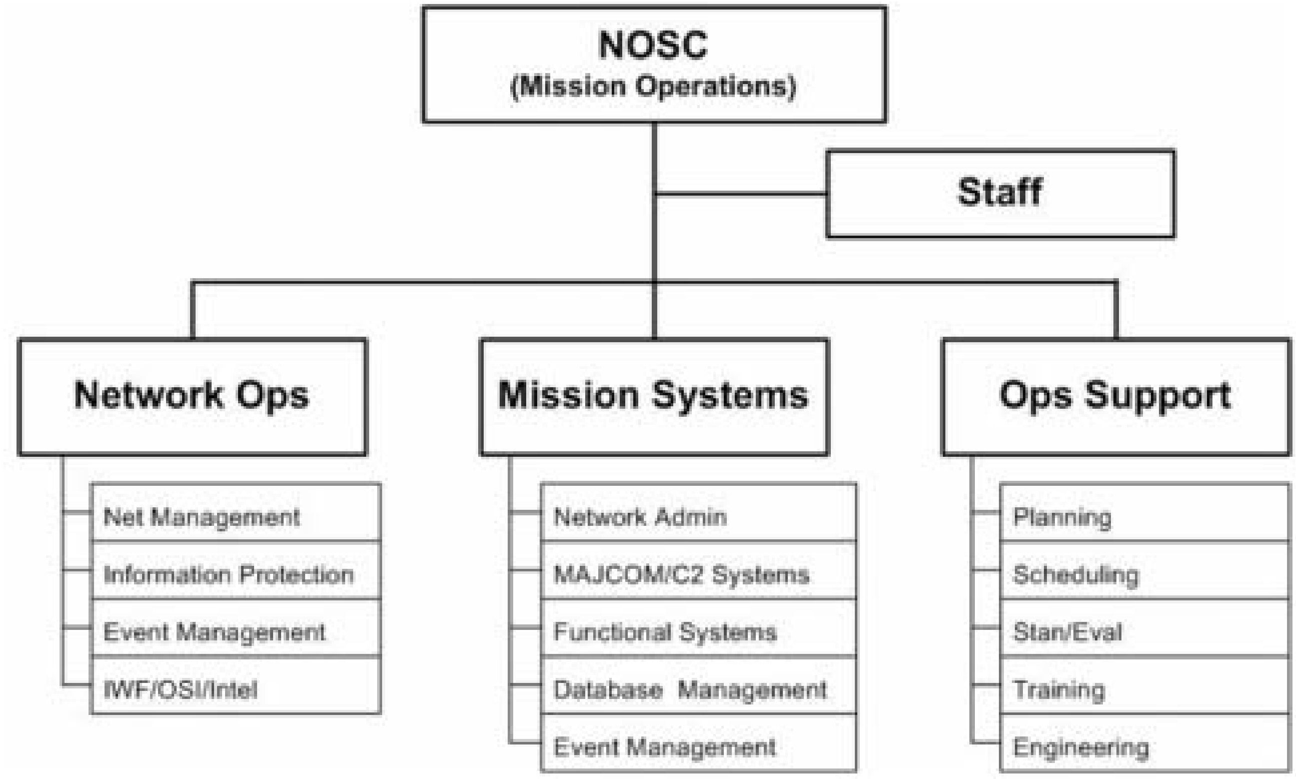
6.1.3.2. This mission area is focused on Assured Resource (Systems and Networks) Availability and on Assured Information Protection. The objectives of this focus are achieved by instituting agile capabilities to resist adversarial attacks, through recognition of such attacks as they are initiated or are progressing, through efficient and effective response actions to counter the attack and safely and securely recover from such attacks; and by reconstituting new capabilities from reserve or reallocated assets when original capabilities are destroyed.

6.2. Network Operations and Security Center (NOSC) Organization.

6.2.1. NOSC Operations. NOSC operations are listed here to provide a standard set of operations that the NOSC provides. NOSC operations are critical to ensuring continuity across the Air Force and to effectively manage the AF-GIG. **Figure 6.1.** depicts the NOSC operations within their respective computer systems squadron (CSS) or communications squadron (CS). It is also possible that these functions may be split across more than one flight within the organization. The Mission Ops area represents the core crew while the Network Ops, Mission Systems, and Ops Support areas represent the supporting functions to the NOSC.

NOTE: **Figure 6.1.** This figure does not depict organizational structure, however, it does capture the functions performed within the organization supporting the NOSC.

Figure 6.1. Network Operations and Security Center (NOSC) Operations.



6.2.1.1. Mission Operations. The Mission Operations element is the core of the NOSC. They are responsible for C2 and maintaining situational awareness over the theater network. They monitor and report on events affecting their theater network. They direct changes to the network in order to ensure a sound network defensive posture and efficient movement of data.

6.2.1.2. Network Operations. The Network Operations element consists of the Network Management, Event Management and Information Protection Operations areas. Event Management incorporates multiple work sections because events happen in all areas. Together Network Operations and Network Management work hand in hand to operate, defend and respond to events that affect the theater network. Additionally, within this element are individuals from the Office of Special Investigations, Intelligence, and Information Warfare Flights.

6.2.1.3. Mission Systems. The Mission Systems element consists of the network administration (NA), database management and event management. These elements provide operating system, application, and messaging administration. They are also responsible for server consolidation efforts and maintaining C2, functional, and theater unique systems. They manage and respond to events with respect to their areas of responsibility. Event management incorporates multiple work sections because events happen in all areas. In other words, the event can be infrastructure related (router down), systems related (server crashed), or even IA related (antivirus needs updated). So in effect event management is everyone's responsibility. Database management generally falls under the Application Services technician's responsibility, but may be contracted out.

6.2.1.4. Operations Support. The Operations Support element provides support to the NOSC in the areas of training, standardization/evaluation, engineering (system integration), planning and scheduling.

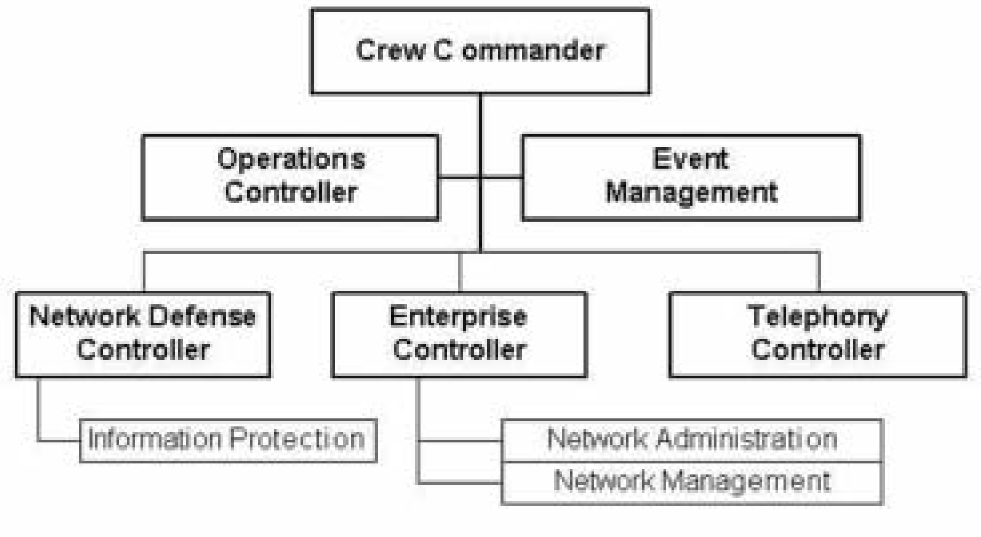
6.3. Crew Positions.

6.3.1. Overview. Crew members coordinate with personnel at their tier or other tiers as necessary in order to provide Core Services to their customers and ensure the availability and security of the AF-GIG. **Attachment 3** identifies the basic crew positions located at each tier of the network hierarchy. Theaters may augment positions to perform specific functions, as required. Crew members will use standardized tools and software approved for Air Force-wide use in the Infostructure Technology Reference Model (i-TRM) and/or the theater DAA. Legacy software tools may also be used, but organizations need to plan how they are going to migrate to the standardized tools.

6.3.2. The original crew position construct was very NCC focused with only four crew positions existing at the theater level. The CSAF mandate for server consolidation and centralized management at the NOSC now requires NCC crew positions to be replicated at the theater level.

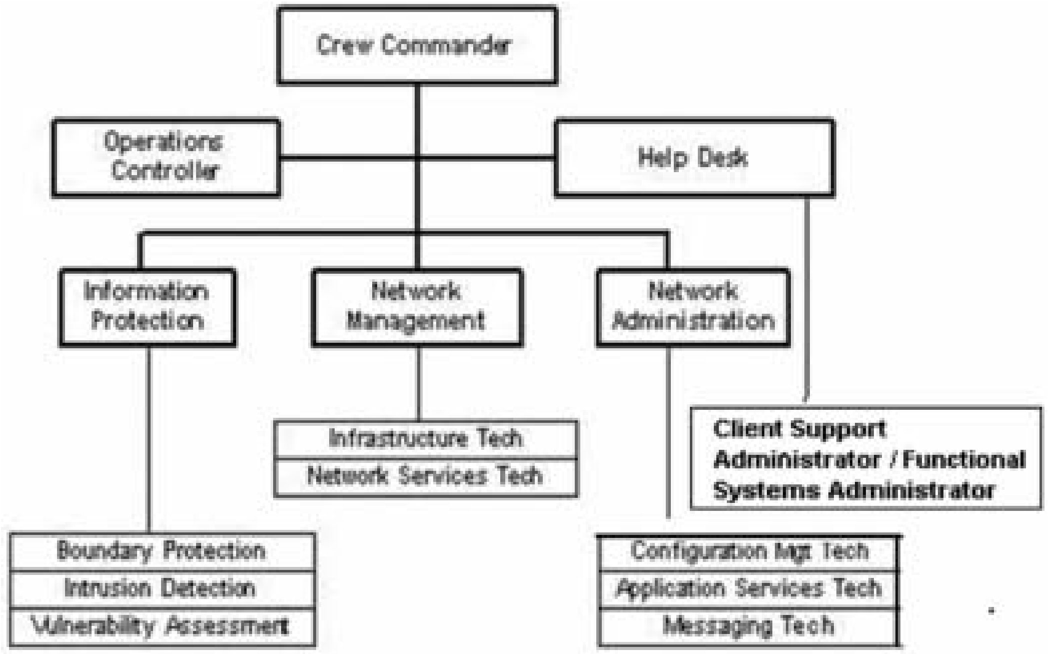
6.3.3. **Figure 6.2.** depicts the crew force relationships within a NOSC. The Crew Commander, Operations Controller, Enterprise Controller, Network Defense Controller, and Voice Controller positions are the foundation of the NOSC. These crew positions monitor and report on events affecting their theater network. Additionally, certain crew positions (Network Defense Controller and Enterprise Controller) direct the actions of those crew positions subordinate to them. The NOSC is responsible for maintaining operational awareness of the entire theater network and conducting situational reporting, coordinating event response and network change implementation as necessary. Event management is also depicted here because events happen in all areas.

Figure 6.2. Network Operations and Security Center (NOSC) Crew Position Structure.



6.3.4. The crew positions within an NCC (see **Figure 6.3.**) are set up similarly to that of the NOSC. Over time, as the NOSC assumes management of NCC resources, the number of personnel required to fill a crew position at the NCC may decrease, but the position will still remain. For example, the difference between an Infrastructure Technician within the NM area of the NOSC, versus NCC, lies in the scope of their responsibilities. The Infrastructure Technician at the NOSC may be responsible for the base's external router and switches, whereas the NCC Infrastructure Technician would be responsible for the vast number of routers and switches within the base network.

Figure 6.3. Network Control Center (NCC) Crew Position Structure.



6.3.5. Crew Position Descriptions. For a complete listing and description of crew positions, please refer to **Attachment 3**.

6.3.6. Training and Certification. Crew members will be certified by position according to AFI 33-115, Volume 2, and Air Force Job Qualification Standards (AFJQS). These establish an Air Force-wide baseline of mandated and enforceable training for network professionals. All individuals filling an Air Force network crew position role are required to be certified in that position. This is not to be confused with commercial certification (Cisco Certified Network Associate [CCNA], Microsoft Certified Engineer [MCSE], etc.). Individuals become Air Force certified by following the procedures set forth in AFI 33-115, Volume 2. All individuals in initial and mission qualification training status must be supervised by an individual certified in the same crew position when performing duties on the AF-GIG. US contractors who provide professional network services (all crew positions) to the Air Force are bound by the requirements stated in contractual agreements. Contractor personnel assigned to perform specific NETOPS tasks are subject to evaluation. All future contracts (including modifications to existing multiyear contracts) for NETOPS tasks, subsequent to this instruction, must cite this instruction and state contractor personnel are subject to evaluation. When results show more training is required, the contract Quality Assurance Evaluator will discuss requirements with the appropriate contracting officer and prepare a proper course of action. AFCA provides a template for contract statements of work on the OPTN web page at **https://private.afca.af.mil/optn**

6.3.6.1. Assigned crew positions at ANG NCC locations will reflect and be tailored to the authorized strength of the unit. Under the current authorized manning, ANG communication units will not be able to fill all the recommended crew positions. Training plans will be adopted to compensate for the availability of assigned personnel during Unit Training Assemblies (UTA). Gaining units should assist upon request, to augment the training and certification of their assigned ANG units.

6.4. Core Services.

6.4.1. Overview. As stated above, Mission Areas are the overarching activities performed by network professionals. NOSC operations are performed by a highly trained and certified crew force consisting of standard crew positions. Core, Functional, and Desktop Services then, are the products provided by our network professionals to the Air Force community and will not be provided by any organization other than the base NCC or supporting NOSC.

6.4.2. Core Services are those services defined by the Air Force IT community as central components of the AF-GIG. They embody the seamless, secure, and reliable transport of timely and trusted information across the AF-GIG.

6.4.2.1. Core services are:

6.4.2.1.1. Electronic Messaging.

6.4.2.1.2. Address Management.

6.4.2.1.3. Directory Services.

6.4.2.1.4. Information Assurance and Security Hardware. (Simple network management protocol [SNMP] monitoring and control of 1) software, 2) bandwidth, and 3) hardware [ports, interfaces, etc.])

6.4.2.1.5. Domain Name Servers (DNS).

6.4.2.1.6. Exchange.

6.4.2.1.7. Windows Internet Naming Service (WINS).

6.4.2.1.8. Domain Controllers (PDC/BDC) remote (PDC/BDC)

6.4.2.1.9. Dynamic Host Control Protocol (DHCP) server.

6.4.2.1.10. Local Directory Service Agent (LDSA).

6.4.2.1.11. Defense Message System (DMS).

6.4.3. Functional services enable the functional workforce(s) to focus on their core competencies. AF-GIG network professionals host functional applications on reliable, secure platforms of AF-GIG servers. Functional applications will be supported by the functional community in accordance with the SLA, MOA, or MOU between the functional organization and the NOSC/NCC. See **Attachment 2** for policy guidance on SLAs.

6.4.4. Desktop services include the common, secure, reliable desktop environment, typically the end-user's interface with the AF-GIG.

6.4.4.1. Desktop Services are:

6.4.4.1.1. Air Force Standard desktop.

6.4.4.1.2. Print services.

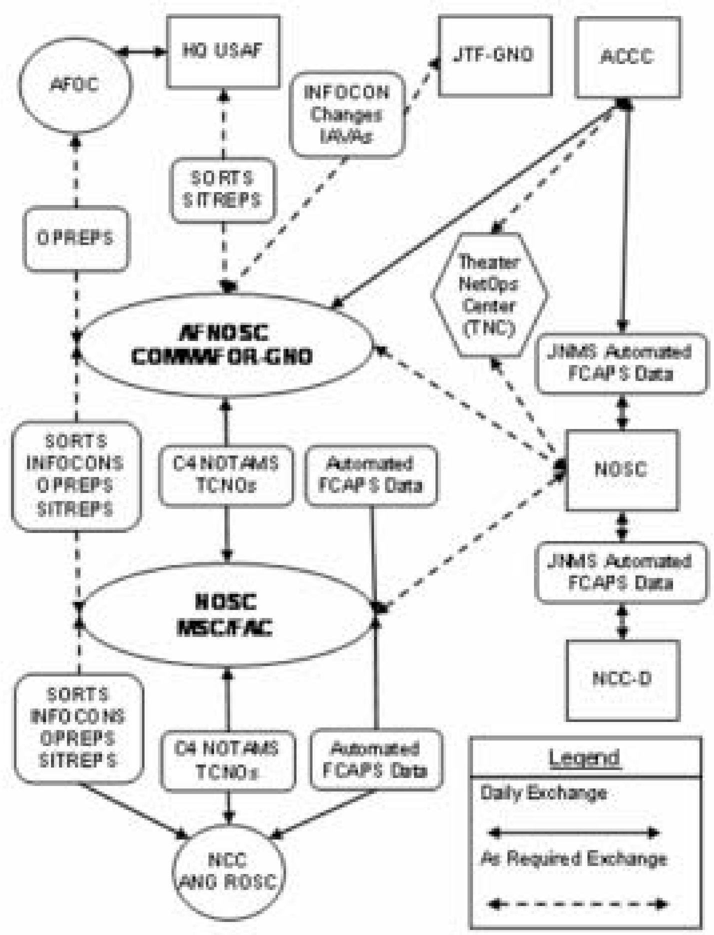
6.4.4.1.3. Standard wireless office automation devices.

Chapter 7

INFORMATION EXCHANGES, RELATIONSHIPS, AND REPORTING

7.1. General. Air Force network operations organizations exchange information internally, between each other, and with external agencies. Information is exchanged to facilitate the maintenance and operation of the AF-GIG, to provide situational awareness, to facilitate integrated Defensive Counter-Information, and to provide commanders with a common operating picture. The picture is developed from information obtained while conducting NETOPS. Generally, the root source of this information comes from "raw" FCAPS data. FCAPS data is monitored, collected, analyzed, processed and reported by the AFNOSC, NOSC, and NCC using software tools that provide a complete view of the AF-GIG. The primary organizations exchanging information are depicted in **Figure 7.1.**

Figure 7.1. Information Exchanges.



7.2. Network Status and Management Reports. Network status and management actions will be reported via scheduled and unscheduled reports. Unscheduled reports focus on the immediate status of the network and are generally tied to events or incidents. Scheduled reports are associated with information exchange and long-term metric analysis.

7.2.1. Reports and Notifications.

7.2.1.1. Information may be exchanged by network operations organizations internally, between each other, and with external agencies using several types of NTOs, reports, and/or notices. OPREP3, SITREP, TCNO, and C4 NOTAM are some examples of these. (***NOTE***: AFNOSC/NOSC/NCCs may pass informational copies of OPREP3s or SITREPs, but the issuing authority for OPREP3s is the wing command post.) Manually reported information completes the data collection function and provides the critical human element in the network equation. The human element and the need for timely, accurate information are essential. NM software could potentially automate some manual exchanges, as long as network professionals still maintain positive control over the AF-GIG.

7.2.1.2. Operational Event/Incident Reports (OPREP3). OPREP3s are reported using operational channels, e.g., Command Posts, to notify commanders immediately of any event or incident that may attract international, national, US Air Force, or significant news media interest. They provide immediate up-channel notification of local network intrusions and probes, INFOCON level changes, and network degradations. They are generally tied to events. An NCC may notify the wing command post of the need to send an OPREP3, and draft the verbiage, but NCCs do not issue OPREP3s. They only forward the draft to the command post and request it be sent. For detailed OPREP3 reporting instructions see AFI 10-206.

7.2.1.3. Situation Report (SITREP). SITREPs are submitted through Command and Control channels and are used to report significant outages. This is a narrative report that keeps addressees informed, and enables higher levels of command to prepare for potential effects of ongoing situations. They are submitted at daily, weekly, or monthly intervals, or as directed. Like OPREP3s, an NCC may notify the wing command post of the need to send a SITREP, and draft the verbiage, but NCCs do not issue SITREPs. They only forward the draft to the wing command post and request it be sent. For detailed SITREP reporting instructions see AFI 10-206.

7.2.1.4. Information Operations Condition (INFOCON). INFOCONs are used to define a defense posture and response based on the status of information systems, military operations, and intelligence assessments of adversary capabilities and intent. The INFOCON system is a DOD methodology providing a structured approach to react and defend against adversarial attacks on DOD computers and telecommunications systems. This is accomplished by directing actions to establish a heightened or reduced defensive IA posture based on assessed threats or hostilities. INFOCON levels are: NORMAL (normal activity), ALPHA (increased risk of attack), BRAVO (specific risk of attack), CHARLIE (limited attack), and DELTA (general attack).

7.2.1.4.1. DOD-wide INFOCONs are declared by the Commander, United States Strategic Command (USSTRATCOM), and disseminated by the JTF-GNO to the COMAFFOR to JTF-GNO via AMHS or voice message. The Air Force-wide INFOCON normally mirrors the DOD-wide INFOCON, but may exceed it if conditions warrant. The Air Force Chief of Staff has delegated the authority to set Air Force-wide INFOCONs to the COMAFFOR to JTF-GNO.

7.2.1.4.2. Official notification for INFOCON changes come through operational reporting channels in the form of INFOCON Change Alert Messages (ICAM), NTOs or OPREP3s. The

NOSCs use TCNOs to implement actions to attain INFOCON protection measures. INFOCON level attainment is officially reported by NCCs using SITREPs through command post channels; it is also reported in response to the NOSCs via C4 NOTAM or TCNO compliance. The SITREP is the official operational report, not the TCNO or C4 NOTAM.

7.2.1.4.3. Theater NOSCs will ensure subordinate bases comply with NTOs, directed INFOCON actions via TCNO and track compliance. AFNOSC will compile an Air Force-wide report and forward it to the COMAFFOR to JTF-GNO as appropriate. Subordinate Air Force units (e.g., MAJCOM, NAF, wing, or base level) may declare a higher INFOCON if local conditions warrant.

7.2.1.5. Time Compliance Network Order (TCNO). TCNOs are downward-directed operations, security, or configuration management-related orders issued by the AFNOSC or theater NOSCs. The TCNO provides a standardized mechanism to issue one "order" **from the AFNOSC to NOSCs/MSCs/NCCs/FACs** directing changes to the AF-GIG. TCNOs do not replace INFOCONs, OPREP3s, SITREPs, or Time Compliance Technical Orders (TCTO).

7.2.1.5.1. TCNOs may be generated internally to direct the implementation of an operational or a security vulnerability risk mitigation procedure or fix action (e.g., software patch), or issued in response to DISA-generated Information Assurance Vulnerability Alerts (IAVA). TCNOs are used to address Air Force or theater wide incidents/problems and not for isolated internal incidents unless impact is determined to be system-wide.

7.2.1.5.2. See AFI 33-138 for TCNO reporting and compliance details and formats.

7.2.1.6. Command, Control, Communications, and Computers Notice to Airmen (C4 NOTAM). C4 NOTAMs are informative in nature and are not used to direct actions. They are used by all organizations within the NETOPS hierarchy. They are the primary means of tracking compliance and disseminating network information that does not require specific actions. However, in some cases, acknowledging receipt of a C4 NOTAM may be required. There are four types of C4 NOTAMs. They are: Informative, Scheduled Event, Unscheduled Event, and Summary. For descriptions of each type of C4 NOTAM and procedures on use refer to AFI 33-138.

7.2.2. Helpdesk, Trouble Resolution and Reporting.

7.2.2.1. The Help Desk is an operation that provides technical information to customers and solves technical problems by providing support and information. The Help Desk should provide an efficient and effective means to answer customers' questions and solve their problems. At the heart of a Help Desk operation is a sophisticated database that contains all the information necessary to handle events. The Help Desk assists the CSA who provides end-user support, an NCC or NOSC working to resolve a network outage, or the AFNOSC providing senior leadership with situational awareness of the AF-GIG. The Help Desk is actually a global repository of information or knows where to retrieve information about customers, vendors, hardware, software, locations, networks, SLAs, problems, and solutions. The database also identifies the interrelationships among these items.

7.2.2.2. The Help Desk will provide network assistance and trouble resolution and will be based on a fully integrated trouble ticketing system. The trouble ticketing system should be able to automatically assign priorities and set response times and escalation timelines based on the criticality of the system being reported on. The trouble ticketing system will be able to share and communicate fix actions across all three network tiers. The Help Desk system should also be integrated with an Automated Call Distribution (ACD) system wherever possible.

7.2.2.3. The Help Desk consists of three different levels. Each of these levels exist at each tier of the Network Operations Hierarchy outlined in **Chapter 2**. These Help Desk levels are:

7.2.2.3.1. Level 1 (CSA). Level 1 support should have end-to-end responsibility for each customer/CSA request. The help desk technician should be empowered to resolve as many requests as possible. Level 1 provides a single point of contact to the customers for servicing a request.

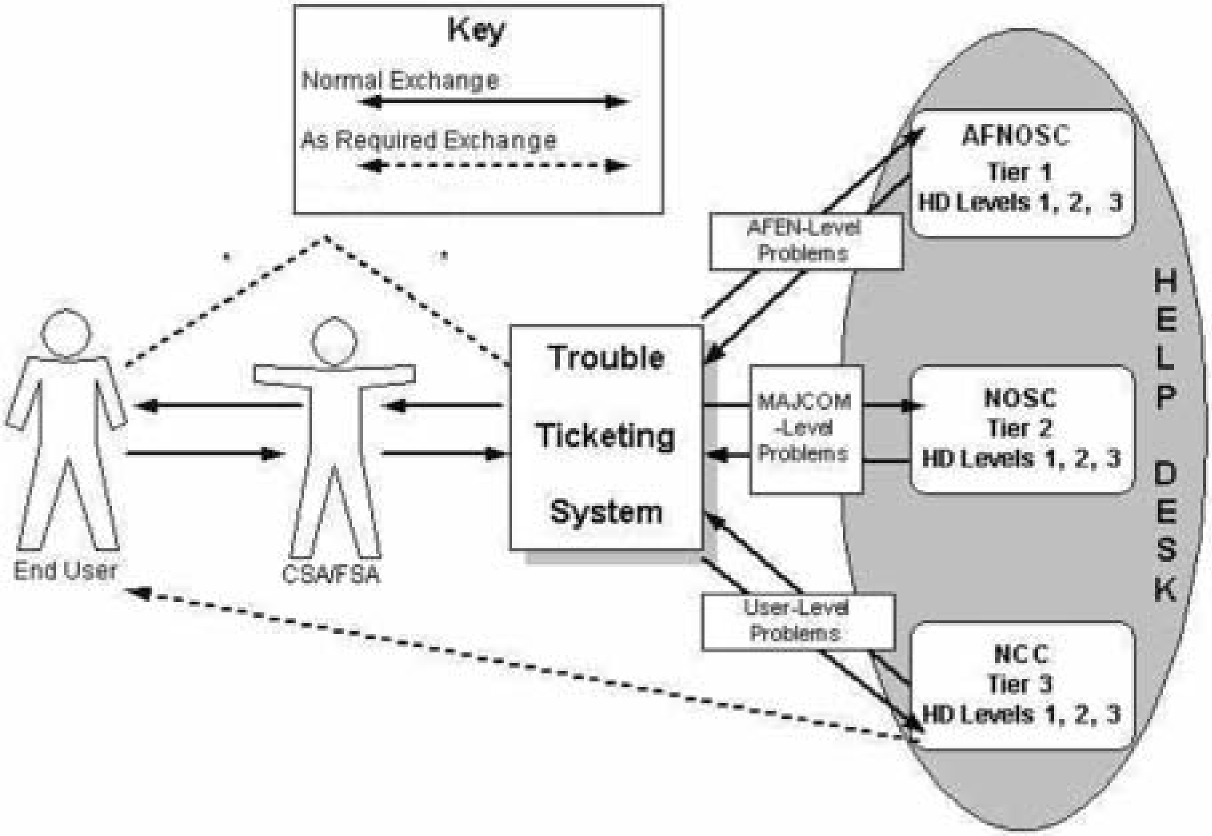
7.2.2.3.2. Level 2 (NCC). Level 2 client support provides advanced technical expertise to Level 1. Their responsibility is to analyze the requests routed to them and resolve the problems. Resources at this level are typically those individuals working in the functional areas outlined in **Attachment 3**.

7.2.2.3.3. Level 3 (NOSC/ANG ROSC). Level 3 support is comprised of highly specialized technical experts. Calls which cannot be solved at Levels 1 and 2 are routed to this level. Resources at this level are typically composed of engineers, system integrators and/or third-party providers/vendors.

7.2.2.3.4. In the absence of a fully automated system, ensure a system is implemented to manually link trouble tickets. An example of how this could be accomplished would be by recording the appropriate ticket number of the organization that has assumed responsibility for the service interruption at each level as the ticket is escalated.

7.2.2.4. Base-level users experiencing problems with network Core Services (see **Chapter 6**) or systems (including common office applications) will first contact their CSA. If the local CSA is unable to fix the trouble, the CSA will enter a trouble ticket into the Help Desk system or contact the Help Desk by phone for ticket submission. CSAs and users will be able to automatically track and view the status of troubles submitted by them. Help Desk personnel will resolve problems by identifying fix actions to the CSA or customer by web interface, E-mail, phone, or by attempting a remote fix action. If local physical access or replacement of equipment is required, the Help Desk will dispatch appropriate base-level personnel. Trouble resolution for many network Core Services or systems will be orchestrated by the regional NOSC Help Desk. The AFNOSC Help Desk will handle all trouble tickets related to all Air Force systems under their control. The trouble resolution process and information exchanges are shown below in **Figure 7.2.**

Figure 7.2. Trouble Ticket Reporting and Tracking.



Chapter 8

AIR FORCE TECHNICAL ORDERS

8.1. General.

8.1.1. The purpose of the Air Force Technical Order (TO) system is to provide concise and clear instructions for safe and effective operation and maintenance of centrally-acquired and managed Air Force military systems. All Air Force personnel are responsible for controlling and using TOs as organizational property in conjunction with official duties. Compliance with Air Force TOs is mandatory.

8.1.2. Technical publications are essential for network support to function properly and to provide the operations activity with accurate information. Technical publications include TOs, commercial manuals, and specialized publications. Set up and maintain these publications according to AFPD 21-3, *Technical Orders,* and 00-5 series technical orders.

8.2. Maintaining Air Force Technical Orders (TO).

8.2.1. Publications Manager.

8.2.1.1. AFNOSC, theater NOSCs, base NCCs, and any other organizations utilizing CITS equipment will appoint a primary and alternate publications manager. This function could be consolidated with Maintenance Support Flight if available as identified in AFI 21-116, *Maintenance Management of Communications-Electronics.*

8.2.1.2. The publications manager will be responsible for:

8.2.1.2.1. Establishing an independent TO account with the base Technical Order Distributing Office (TODO). Ensure that the account is on requirement for all the TOs and any associated TCTOs.

8.2.1.2.2. Maintaining those TOs required for support of all CITS equipment. Maintain additional TOs required for training and deploying.

8.2.1.2.3. Ensuring TOs are adequate, accurate and readily available to Network Professionals (TO 00-5-1, *Air Force Technical Order System*) and maintaining sufficient requirement to support operational load. TOs should not be removed from the primary work locations simply to accommodate the staff.

8.2.1.2.4. Identifying any errors, contradictions, or procedures requiring clarification, by following specific procedures in TO 00-5-1. See TO 00-5-1 for specific guidance on preparing AFTO IMT 22, **Technical Manual (TM) Change Recommendation and Reply**.

8.2.1.2.5. Ensuring TCTOs are managed and issued in accordance with procedures in TO 00-5-15, *Air Force Time Compliance Technical Order Process*. TCTOs are military orders issued by order of the Secretary of the Air Force and as such, shall be complied with as specified in the TCTO.

8.2.1.2.6. Utilizing AFMQCC 200-6 (current version) Technical Order Control Check Sheet and other applicable guidance to aid units in maintaining technical order programs.

Chapter 9

MANAGING COMPUTER AND NETWORK EQUIPMENT MAINTENANCE CONTRACTS AND WARRANTIES

9.1. General.

9.1.1. Air Force organizations at all levels of the AF-GIG NETOPS hierarchy are responsible for the sustainment of computer and network equipment. Sustainment includes acquisition of spare parts, contract maintenance and warranty management. A Logistics Support Plan should be developed as described in AFI 21-116 to ensure sustainment of new and existing computer and network systems. This chapter provides guidance on determining the quantity/types of spares to purchase as well as maintenance and warranty management requirements for all organizations that operate and maintain computer and network equipment. This chapter is not intended to replace or duplicate guidance found in other AFIs (e.g., AFI 21-116 or AFI 33-112) but merely provides guidance to ensure there is a logical process in place to determine the quantities/types of spares required to sustain the computer or network equipment. Additional guidance is provided to ensure computer and network equipment maintenance contracts and warranties are managed in the most cost efficient manner.

9.2. Acquisition of Spares.

9.2.1. A Logistics Support Plan will be developed according to AFI 21-116 by AFNOSC/NOSC/NCC personnel or other organizations that operate and maintain computer and network equipment. The Logistics Support Plan will be used to determine the quantity of operational spares to be maintained on-hand. When developing the plan, consider technical information such as: reliability data from the manufacturer; order and shipping time; and mean time between failure rates. Network personnel should also consider mission impact factors such as whether the item is a single point failure item and/or is mission critical. Ultimately it is the commander's decision, based on past experience with low density/commercial off-the-shelf (COTS) systems, that determine the quantity of on-hand operational spares required to ensure mission accomplishment. However, the method or rationale used to determine the quantity of on-hand operational spares must be documented in the Logistics Support Plan as specified in AFI 21-116.

9.2.2. Special consideration should be given to the quantity of access layer switches to maintain as operational spares. It will be at the discretion of the Communication System Officer (CSO), in conjunction with the commander, to determine the number of uninstalled access layer switches to keep in the inventory as backups.

9.2.3. Units will track equipment downtime by equipment item. The downtime information along with reliability data obtained from the manufacturer can be used as determining factors when computing operational spares requirements.

9.3. Equipment Identification.

9.3.1. AFNOSC/NOSC/NCC personnel or any other organizations that operate and maintain computer and network equipment will comply with AFI 33-112 as it pertains to equipment identification and accountability

9.3.2. All computer and network equipment will be categorized as installed, operational spare, or available excess in Information Technology Asset Management (ITAM). Validate ITAM status codes during inventories and update as equipment status changes. An operational spare is a piece of serviceable equipment required to sustain operations in the interval between ordering and replenishment. This equipment has the latest operating system version, security patches, and quality of service enhancements already loaded and facilitates "plug and play" (PnP) replacement. Equipment assets that are not installed on a system or identified as an operational spare will be identified as available excess in ITAM. Equipment identified as excess in ITAM will be made available to other Air Force installations or turned in to Defense Reutilization and Marketing Office (DRMO).

9.3.3. All uninstalled backbone and WAN switches will be identified as operational spares and not identified as excess in ITAM.

9.4. Maintenance Contract and Warranty Plan.

9.4.1. Evaluate all maintenance options included in the technical solution to determine the most cost-effective coverage prior to selecting a maintenance option. When possible, utilize only one maintenance option per equipment item. Network personnel (for locally purchased) or PMO for (centrally managed equipment) will obtain equipment reliability data from the manufacturer as part of the technical solution process. In addition, evaluate the cost of all maintenance alternatives before exercising options to extend existing maintenance contracts or placing equipment on maintenance contracts at the end of warranty periods. During the evaluation, identify and exclude highly reliable equipment from maintenance contracts when possible. Consider entire life cycle costs in making this analysis--not just the initial acquisition and first 1-2 years costs.

9.4.1.1. Network personnel validate operational and fiscal needs before ordering contracted maintenance on network and computer systems. Network personnel will establish a conscientious contract management plan to track equipment warranty information to ensure contract maintenance funds are not used to repair equipment already under warranty.

9.4.1.2. All organizations will record and track equipment warranty information using the SAF/XCIAS created Contract Maintenance and Warranty Plan database. This database can be downloaded from the AFCA Maintenance and Supply web site, **https://private.afca.af.mil/c-e_maint/** , **https://private.afca.af.mil/supply/**.

9.4.1.3. Network personnel must conduct thorough research to determine the feasibility of including or excluding highly reliable, access layer switches from maintenance contracts. Under no circumstance should access layer switches coded as operational spares or excess, be included in maintenance contracts. It will be the discretion of the CSO to determine the number of uninstalled access layer switches to keep in the inventory as operational spares.

9.4.1.4. Backbone switches and routers that provide inter-building and WAN connectivity should be added to maintenance contracts to ensure current operating system and security patches are authorized and applied.

9.4.1.5. Backbone switches and routers that provide interbuilding and WAN connectivity should be added to maintenance contracts to ensure current operating system and security patches are authorized (unless already covered under existing Air Force contracts such as CITS Life Cycle Support). The commander always retains the authority to include specific critical items on maintenance contracts to ensure operational network reliability. However, if the decision is made to include highly reliable assets or assets already under warranty in a maintenance contact, the unit should be prepared to justify the decision and the reasons should be thoroughly documented.

9.4.1.6. Refer to AFI 33-202, Volume 1, and the Air Force systems security instruction (AFSSI) and manual (AFSSM) 5000-series publications (**https://www.afca.scott.af.mil/ip**) for guidance on managing maintenance contracts for systems that process classified information.

9.5. Uninstalled Equipment.

9.5.1. Uninstalled equipment is defined as operational spares and equipment that have been identified as excess. Units will maintain a list of uninstalled network equipment and must review the list prior to purchasing additional equipment. Uninstalled equipment should also be used to satisfy new approved requirements whenever possible.

Chapter 10

VULNERABILITY ASSESSMENT TOOLS

10.1. General.

10.1.1. The CITS Enterprise Network Support Center (ENSC) at HQ SSG/DOYN is chartered by the CITS Program Management Office, HQ ESC/NI, to provide 24/7 technical support to CITS NBM/ND users worldwide.

10.1.2. In addition to providing technical support, the CITS ENSC is tasked to provide Vulnerability Assessment Tool (VAT) license keys to all NCCs equipped with the CITS NBM/ND suite, as well as to theater NOSCs. Once the VAT license key has been issued, the base/theater SC (or A6) will exercise the authority and responsibility for its use.

10.1.3. Other Air Force entities may have the need to request license keys for VATs. Once a VAT license key request is approved and key issued, the cognizant authority will exercise this authority and assume responsibility for usage. This chapter establishes procedures and responsibilities for NCC, NOSC, CITS ENSC and all other personnel.

10.2. Vulnerability Assessment Tools (VAT) License Key Request Procedures.

10.2.1. NCC. The base-level communications unit commander (SC), who is the cognizant authority for the base installation NCC, will request the VAT license key from the CITS ENSC. When there are multiple base-level SCs (e.g., host-tenant environments), tenant SCs will forward key request through the host command's SC, who will then forward to the ENSC. ANG or Air Force Reserve tenant sites that are not located on an active duty base may request their own license keys from the respective ANG or Reserve base-level SC. DRU/FOA/MSCs that do not fall within the host-tenant environment may request their own license keys from the CITS ENSC.

10.2.2. NOSC. The theater SC or NOSC chief/deputy (when acting on behalf of the theater SC) is the cognizant authority for the theater NOSC and will request the VAT license key. Initial key requests can be forwarded directly to the CITS ENSC.

10.2.3. All Other Requests. This category refers to Air Force organizations not residing on an Air Force base or Air Force tenants who are not serviced by the base NCC. Only the individual who is the cognizant authority for the base tenant or Air Force organization may request the VAT license key. Air Force tenants residing on an Air Force base, but not serviced by the base NCC, will forward their request to the base-level communications unit commander (SC), who is the cognizant authority for the base installation NCC. Air Force organizations not residing on an Air Force base will forward the key requests directly to the ENSC CITS Help Desk equivalent of the owner of the network and request an internet security systems (ISS) internet scanner Key from that entity

10.3. Training and Affidavits.

10.3.1. All Vulnerability Assessment Specialists (VAS) must be trained according to paragraph **10.3.2.** These are the only individuals authorized to perform vulnerability assessment scans.

10.3.2. Training must be provided by an approved Air Force/MAJCOM sponsored IP tools course or "through the use of on the job training (OJT)" by an individual who was trained on the VAT at an approved Air Force sponsored instructor-led IP tools course. The person conducting the training must have attended an Air Force approved instructor-led course and have the training certificate on file in their AF Form 623, **Individual Training Record Folder**. Personnel receiving training through OJT must have a copy of the signed training affidavit filed in their OJT records. (See **Attachment 4** for affidavit example).

10.4. Key Requests and Renewals.

10.4.1. All key requests will be requested on official Air Force letterhead as described below and in **Attachment 4**. When issued, the key will be set to expire in 180 days for security and risk mitigation reasons, unless issued as a special one time key according to paragraph **10.4.5.** Typically, keys expire every June 30th and December 31st. Key renewal requests should be submitted at least 4 weeks prior to key expiration, as the CITS ENSC will not automatically send the replacement key. Additionally, new letters must be sent each 6 months. The request letter can be mailed or faxed to the CITS ENSC at:

HQ OSSG/SWSN

ATTN: CITS ENSC INFORMATION SYSTEM SECURITY (ISS) KEY AGENT

10 Baker Street

Maxwell AFB-Gunter Annex AL 36114

FAX (334) 416-3377, DSN 596-3377

Voice (334) 416-5771, DSN 596-5771 option 2,1,9

10.4.2. The ENSC will only issue renewal keys to persons holding valid formal training credentials from an Air Force approved instructor-led course. Cognizant authorities must ensure at least one formally trained VAS is assigned to the NCC/NOSC at all times (preferably two).

10.4.3. Provide the request type, IP address range and complete mailing address as follows (**Table 10.1.**):

Table 10.1. Key Requests and Renewals.

Request Type:	[Initial -or- Replacement]
Specify VAT key IP Address Range(s):	xxx.yy.0.0 - xxx.yy.255.255 (Example)
Complete Mailing Address:	[Provide the complete VAS name and mailing address, including building and room number]

10.4.4. Provide the base-level SC point of contact (POC) and telephone number.

10.4.5. Special Requests. A special one-time key may be requested for a special project, e.g., conduct of Security Test and Evaluation (ST&E), deployment of information system for mission accomplishment or exercise, conduct of C&A effort when not supported by base NCC, etc. Special one-time keys will be issued with a key life of 10, 30, 60, or 90 days. Special one-time key requests require the same request submission and training requirements as other key requests.

10.4.6. Deviations to key request procedures because of inability to meet training, certification, or other requirements will be forwarded by ENSC to HQ AFCA/CAFT for resolution.

10.5. Combat Information Transport System (CITS) ENSC Procedures.

10.5.1. The appointed VAT Key Agents will be the individuals that will actually cut the license key and are responsible to ensure compliance with this procedure. The appointment letters will be kept current and maintained by ENSC.

10.5.2. Upon receipt of the written key request, the ENSC will verify its authenticity and ensure all pertinent information is provided according to paragraph **10.3.** and **Attachment 4**. After verification, the ENSC will cut the key for the specified IP domain range with a default expiration date of 180 days and place it in removable media. The ENSC will maintain the original key request letter and the ENSC response for tracking purposes.

10.5.3. The ISS license key disk may be mailed using US certified mail. The address shall contain the VAS name as a part of recipient address. Emergency key requests can be delivered by overnight mail when it has been prepaid, and requester has arranged pickup. Keys will not be E-mailed. The VAS name(s) will be provided to applicable NOSC upon request.

10.5.3.1. In order to improve response time and save Air Force funds, ENSC will use their secure web site (**https://support.cits.lab.gunter.af.mil**). This is a UNIX-based site with secure sockets layer (SSL) enabled that performs a DNS forward and reverse lookup to ensure that users are on the Air Force network. Additionally, ENSC will only load the keys to this server after the official request. Users will only have read permissions to download the keys. Immediately after confirming their download, ENSC will remove the key from the server.

Chapter 11

SIMPLE NETWORK MANAGEMENT PROTOCOL MANAGEMENT

11.1. General.

11.1.1. Simple Network Management Protocol (SNMP) is often used to remotely configure network devices. SNMP Community strings act as passwords and are used to authenticate management traffic sent to a managed device from a management station.

11.1.2. Most equipment is shipped with public, private and/or factory default community strings configured. These community strings must be changed to prevent unauthorized access.

11.2. Minimum Simple Network Management Protocol (SNMP) Community String Requirements.

11.2.1. Each community string must contain a minimum of eight characters comprised of at least one uppercase character, one lowercase character, one number, and one special character (!@$%^&*, etc.). Do not use the # special character since some software programs may interpret any characters preceded by the # as a comment. Modify systems unable to support eight character community strings at the earliest and most cost-effective opportunity. In the interim, use the maximum number of characters the system is capable of supporting. Configure SNMP agents to send traps to, or accept packets from, only authorized hosts. Where technically applicable, implementation of SNMPv3 is highly recommended.

11.2.2. Community strings will not contain dictionary words spelled forward, backward, or split with a number or special character. Community strings will not contain the machine name, base name or any other easily decipherable phrase. Public (read) and private (set) strings will not be set to the same value.

11.2.3. Change community strings every 90 days according to AFMAN 33-223. Also change community strings when personnel with knowledge of the community strings are permanently transferred to another location or terminate employment. Ensure procedures are in place so the affected NCC, NOSC, CSA, and FSA are notified when an employee (military, civilian, or contractor) transfers, retires, separates, or is terminated. Global strings will not be used; separate strings will be used for logical divisions of network.

11.3. Simple Network Management Protocol (SNMP) and Network Management.

11.3.1. NCC will perform network management monitoring on all equipment operated or maintained by the NCC. When technically possible enable SNMP on all AF-GIG infrastructure devices, network management servers, security management servers, web proxy servers, firewalls, DNS servers, domain controllers, DHCP servers, and Active Directory servers. Ensure that SNMP connectivity between NCC, ANG ROSC, and NOSC is fully functional.

11.3.2. NOSC will perform network management monitoring on all equipment operated or maintained by NOSC. When technically possible enable SNMP on all AF-GIG infrastructure devices, network management servers, security management servers, web proxy servers, firewalls, DNS servers, domain controllers, DHCP servers, and Active Directory servers. Ensure that SNMP connectivity between NCC and NOSC is fully functional.

11.3.3. When technically possible, NOSCs will develop and enable access control lists or other methods to prevent unauthorized read and write privileges from illicit or rogue management stations.

11.3.3.1. Disable or remove SNMP on devices if not managed (e.g., printers, plotters, print servers, workstations, etc.) when technically possible.

11.3.3.2. Ensure SNMP vulnerability scans are run monthly within the theater using vulnerability assessment tools to analyze base networks under NOSC/NCC control.

Chapter 12

DOMAIN NAME SERVICE MANAGEMENT

12.1. General.

12.1.1. Domain Name Service (DNS) is a critical part of AF-GIG that associates IP addresses to host names. The DNS naming convention impacts not only all three NETOPS tiers, but also has the potential to impact addresses/host names across the DOD. This fact necessitates the standardization of DNS administration throughout the AF-GIG. This chapter provides guidance and procedures to ensure the naming convention maintains a hierarchical structure. A hierarchical structure is provided that maximizes the ability to comply with AFNOSC advisories, protect Air Force domains and provide a standard for Air Force messaging configuration and delivery.

12.1.2. The DNS policy described within the chapter applies to external DNS (base/majcom.af.mil) hierarchy only and not to the internal Active Directory naming standards (base.majcom.ds.af.mil).

12.2. Air Force-Level Domain Name Service (DNS).

12.2.1. The AFNOSC is the top of the Air Force enterprise DNS hierarchy and the only authorized Air Force point-of-contact to internet DNS registries. The NIC assigns blocks of IP addresses to the AFSN Program Management Office. AFSN manages the IP addresses and reassigns the IP addresses to Air Force users.

12.2.2. All correspondence and issues with the NIC pertaining to af.mil templates, DISN host, and specific user templates shall be processed through the AFNOSC. The specific user templates processed through the AFNOSC pertain to modifications on previously registered networks and point-of-contact (technical and/or administrative) for domains, DISN host and IP addresses. All other user templates, correspondence and issues with the NIC pertaining to IP registration shall be processed through AFSN. The user will maintain a valid record in the locally generated database of who is authorized (WHOIS) database at the NIC.

12.3. Air Force Third-Level Domain Name Service (DNS).

12.3.1. Air Force Third Level (e.g., basename.af.mil) Domains. Only bases are eligible to register a third level domain under af.mil. Third level domain names will not be used for Air Force organizations. All other DOD organizations will register through their respective second level domain administrators using the registration procedures established by those offices. Ensure that SNMP connectivity between NCC and NOSC is fully functional. The only exceptions are MAJCOM-name.af.mil and **www.af.mil**.

12.3.2. Third level domains must reside on a minimum of two (2) domain name servers, be a part of the '.mil' domain, and be on a network registered with the DOD NIC. Ensure that SNMP connectivity between NCC and NOSC is fully functional.

12.3.2.1. Registration is coordinated through the AFNOSC and a point-of-contact list will be maintained at the AFNOSC. Technical and administrative points-of-contact for the domain, the domain name, and its name servers must be registered with the DOD NIC.

12.4. DNS Management Requirements.

12.4.1. All DNS servers must:

12.4.1.1. Reside on a network that has ‘in-addr’ (reverse domain name) service.

12.4.1.2. Be protected by a firewall or filtering router which permits only DNS queries from appropriate clients and appropriate zone transfers to other name servers. Under current CITS guidelines, the external DNS sits outside of the base (Tier 3) firewall. However, the DNS server could be moved to a screened subnet (third burb) off of the firewall and still be afforded the required protection.

12.4.1.3. Be located in a room that has positive access control.

12.4.1.4. Be protected by an Uninterruptible Power System (UPS) or backup power supply.

12.4.1.5. Allow domain transfer only between master and slave name servers and only run the DNS service on the name servers. All other unnecessary services (e.g., http, ftp, telnet, send mail, NetBIOS, etc.) will be turned off on the name servers.

12.4.1.6. Include for each domain a Start of Authority (SOA) record containing an administrator E-mail address. E-mail address will match the format of “hostmaster@domain” (e.g., hostmaster@usafe.af.mil).

12.4.1.7. Ensure access accounts on the name servers are limited to the domain administrators at the base communications squadron/NOSC and have the latest AFNOSC approved secure version of DNS/Berkeley Internet Name Domain (BIND).

12.5. Exceptions to Domain Name Service (DNS) Management Policy.

12.5.1. Exceptions to this guidance will be staffed through the organization's parent command/organization to SAF/XCIF with info copy to HQ AFCA/ECFP, for evaluation and approval/disapproval. The request must describe the following: the scope of the mission, the function performed, the customers serviced by the organization and justification for a nonstandard domain name rather than using that of their parent command.

12.5.2. A copy of the approval/disapproval will be filed with the record set of the publication at HQ AFCA/ECFP. The exception remains in effect until this publication is revised, or the approving official cancels it in writing. Once the publication is revised the requester must renew the exception.

Chapter 13

SERVICE LEVEL AGREEMENTS, MEMORANDUM OF AGREEMENT, MEMORANDUM OF UNDERSTANDING

13.1. Service Level Agreements (SLA), Memorandums of Agreement (MOA), Memorandums of Understanding (MOU). The NCC or NOSC will establish SLAs, MOAs/MOUs as appropriate, with customers whose network support requirements exceed the core services defined in paragraph **6.4.** or the Air Force IT service defined by the AF-CIO. SLAs define division of responsibilities for network operations and services to minimize duplication of effort between organizations. MOAs and MOUs define the resources each party will provide to support delivery of negotiated services. SLAs quantify the level of support for the services defined in a MOA or MOU. Whenever possible, SLAs will identify the minimum levels of support required by the users rather than acceptable failure rates (uptime rates as opposed to downtime rates). SLAs will also describe the prioritization of systems and services included in the SLA. A master SLA may be necessary for large/complex functions with multiple system SLAs. See **Attachment 2** for a sample SLA, MOA/MOU.

13.2. NOSC, ANG ROSC and NCCs. An MOA/MOU must be established and maintained between the NOSC, ANG ROSC and their NCCs to fully diagram the core systems managed by the NOSC at the respective bases and the level of service to be expected.

Chapter 14

INFORMATION COLLECTIONS, RECORDS, AND FORMS OR INFORMATION MANAGEMENT TOOLS (IMT)

14.1. Information Collections, Records, and Forms or Information Management Tools (IMT).

14.1.1. Information Collections. No information collections are created by this publication.

14.1.2. Records. Records pertaining to operational capability reporting are created by this publication. Retain and dispose of these records according to AFRIMS RDS, Table 11-4 (will become Table 10-16), located at **https://afrims.amc.af.mil/rds_series.cfm**.

14.1.3. Forms or IMTs (Adopted and Prescribed).

14.1.3.1. Adopted Forms or IMTs. DD Form 250, **Material Inspection and Receiving Report**; DD Form 1368, **Modified Use of Leased Communication Facilities;** AF Form 623, **Individual Training Record Folder;** AF IMT 723, **SORTS DOC Statement**; AF IMT 847, **Recommendation for Change of Publications**; AF IMT 1261, **Communications and Information Systems Acceptance Certificate; and** AFTO IMT 22, **Technical Manual (TM) Change Recommendation and Reply.**

14.1.3.2. Prescribed Forms or IMTs. No forms or IMTs are prescribed by this publication.

MICHAEL W. PETERSON, Lt, Gen, USAF
Chief, Warfighting Integration and Chief Information Officer

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Clinger-Cohen Act of 1996

ACP 121/US-SUP-1, (C) *Communication Instruction General* (U)

DODI 4630.8, *Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)*, June 30, 2004

DOD 5200.2-R, *Personnel Security Program*, January 1987 w/Change 1, February 12, 1990; Change 2, July 14, 1993, and Change 3, February 23, 1996

DODD 8100.1, *Global Information Grid (GIG) Overarching Policy,* September 19, 2002

DODI 8500.2, *Information Assurance (IA) Implementation*, February 6, 2003

DISAC 300-175-9, *DCS Operating Maintenance Electrical Performance Standards*

CJCSI 6212.01D, *Interoperability and Supportability of Information Technology and National Security Systems,* 8 March 2006

AFPD 21-3, *Technical Orders*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems* (will become Information Resources Management)

AFI 10-206, *Operational Reporting*

AFI 10-901, *Lead Operating Command—Communications and Information Systems Management*

AFI 21-116, *Maintenance Management of Communications-Electronics*

AFI 33-103, *Requirements Development and Processing*

AFI 33-108, *Compatibility, Interoperability, and Integration of Command, Control, Communications and Computer (C4) Systems* (will become Interoperability and Supportability of Information Technology and National Security Systems)

AFI 33-112, *Computer Systems Management* (will become Information Technology Asset Management (ITAM)

AFI 33-114, *Software Management*

AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals* (will become Network Operations Training and Standards)

AFI 33-119, *Air Force Messaging*

AFI 33-129, *Web Management and Internet Use*

AFI 33-138, *Enterprise Network Operations Notification and Tracking*

AFI 33-202, Volume 1, *Network and Computer Security*

AFI 33-202, Volume 6, *Identity Management*

AFI 33-207, *Computer Security Assistance Program*

AFI 33-219, *Telecommunication Monitoring and Assessment Program (TMAP)*

AFMAN 33-223, *Identification and Authentication*

AFI 36-2201, Volume 3, *Air Force Training Program, On The Job Training Administration*

AFCAT 36-2223, *USAF Formal Schools*

AFMAN 37-123, *Management of Records* (will become AFMAN 33-363)

AFI 64-117, *Air Force Government-Wide Purchase Card (GPC) Program*

AFI 65-601, Volume 1, *Budget Guidance and Procedures*

TO 00-5-1, *Air Force Technical Order System*

TO 00-5-15, *Air Force Time Compliance Technical Order Process*

Abbreviations and Acronyms

ACCC—Air Communications Control Center

AEF—Air Expeditionary Forces

AETC—Air Education and Training Command

AF—Air Force (Forms and IMTs Only)

AF-GIG—Air Force-Global Information Grid

AFC2ISRC—Air Force Command and Control & Intelligence, Surveillance, and Reconnaissance Center

AFCA—Air Force Communications Agency

AF-CIO—Air Force Chief Information Officer

AFEN—Air Force Enterprise Network

AFFOR—Air Force Forces

AFI—Air Force instruction

AFIWC—Air Force Information Warfare Center

AFJQS—Air Force job qualification standard

AFMAN—Air Force manual

AFMC—Air Force Materiel Command

AFNETOPS—Air Force network operations

AFNOSC—Air Force Network Operations and Security Center

AFOSI—Air Force Office of Special Investigations

AFPCA—Air Force Pentagon Communications Agency

AFPD—Air Force policy directive

AFSC—Air Force specialty code

AFSN—Air Force systems network

AMC—Air Mobility Command

AMHS—Automated Mail Handling System

ANG—Air National Guard

AOR—area of responsibility

ASIM—automated security incident measurement

AFSSI—Air Force systems security instruction

AFSSM—Air Force systems security manual

ATCALS—Air Traffic Control and Landing Systems

C2—command and control

C4—command, control, communications, and computers

C&A—certification and accreditation

CITS—Combat Information Transport System

COMAFFOR—Commander, Air Force Forces

CS—communications squadron

CSA—client support administrator

CSAF—Chief of Staff of the Air Force

CSS—computer systems squadron

CSO—Communication Systems Officer

DAA—designated approving authority

DCI—defensive counter-information

DCS—Defense Communications System

DECC—Defense Enterprise Computer Center

DHCP—dynamic host configuration protocol

DII—defense information infrastructure

DIICC—defense information infrastructure control concept

DIRLAUTH—direct liaison authority

DISA—Defense Information Systems Agency

DISN—Defense Information Systems Network

DITCO—Defense Information Technology Contracting Office

DNS—domain name service

DOC—designed operational capability

DOD—Department of Defense

DRU—direct reporting unit

DSN—defense switched network

EC—equipment custodian

ECPA—Electronic Communications Privacy Act

EI—engineering and installation

EITDR—Enterprise Information Technology Data Repository

ENSC—Enterprise Network Support Center

ETM—Enterprise Telephony Management

FAC—functional awareness cell

FOA—field operating agency

FOC—final operating capability

FCAPS—fault, configuration, accounting, performance, and security

FSA—functional system administrator

FWA—fraud, waste, and abuse

GAL—global address list

GCCS—Global Command and Control System

GIG—global information grid

GNO—global network operations

GNOSC—global NOSC

GPS—Global Positioning System

GSU—geographically separated unit

IA—information assurance

IAC—Infrastructure Architecture Council

IAVA—information assurance vulnerability alerts

IDM—information dissemination management

INFOCON—information operations condition

I-NOSC—Integrated Network Operations and Security Center

IP—internet protocol

I-Plan—implementation plan

IPO—information protection operations

IQT—initial qualification training

ISP—information support plan

IS—information systems

ISS—information systems security

ISSO—information systems security officer

IT—information technology

ITAM—information technology asset management

ITIL—Information Technology Infrastructure Library

i-TRM—infostructure technology reference model

JCCC—Joint Communications Control Center

JNMS—Joint Network Management System

JTF—Joint Task Force

LAN—local area network

LRU—line replaceable unit

MAJCOM—major command

MAN—metropolitan area network

MECL—minimum essential circuit listing

MOA—memorandum of agreement

MOU—memorandum of understanding

MSC—Mission Support Center

MTBF—Mean Time Between Failure

NA—network administration

NOD—Network Operations Division

NAF—Numbered Air Force

NCC—Network Control Center

ND—Network defense

NETCOP—network common operating picture

NETOPS—network operations

NetA—network attack

NetD—network defense

NIC—Network Interface Card

NIPRNET—non-secure internet protocol router network

NM—network management

NBM/ND—network battle management / network defense

NOSC—Network Operations and Security Center

NOTAM—notice to airmen

NTP—network time protocol

NTO—NETOPS tasking order

OJT—on the job training

OPCON—operational control

OPREP—operational report

OPREP3—operational event/incident reports

OPTN—operationalizing and professionalizing the network

O&ST—order and shipping time

ORM—operational risk management

PKI—public key infrastructure

PMI—preventive maintenance inspection

PMO—program management office

POC—point of contact

POM—Program Objective Memorandum

PSCF—Primary Systems Control Facility

QC—quality control

QoS—quality of service

RDS—Records Disposition Schedule

ROE—rules of engagement

ROSC—Regional Operations and Security Center

S&NM—systems and network management

SDP—service delivery point

SECAF—Secretary of the Air Force

SIPRNET—secret internet protocol router network

SITREP—situation report

SMTP—simple mail transfer protocol

SNMP—simple network management protocol

SLA—service level agreement

SOA—start of authority

SORTS—Status of Resources and Training System

SPO—system program office

SYSCON—systems control

TAC-IP—tactical internet protocol

TACON—tactical control

TCNO—time compliance network order

TCTO—time compliance technical order

TMAP—Telecommunications Monitoring and Assessment Program

TO—technical order

TODO—Technical Order Distributing Office

TTP—tactics, techniques, and procedures

UPS—Uninterruptible Power System

UTA—unit training assemblies

VAS—vulnerability assessment specialists

VAT—vulnerability assessment tool

VoIP—voice over internet protocol

VPN—virtual private network

VPS—Voice Protection System

WAN—wide area network

WFHQ—warfighting headquarters

WHOIS—locally generated database of who is authorized

WLAN—wireless local area network

Terms

Backdoor—Data circuit that does not pass through a hardware level firewall prior to entering the local base.

Combat Information Transport System (CITS)—Program managing the life cycle of infostructure systems. Life cycle management includes acquisition, sustainment, implementation, and maintenance activities. CITS is composed of four systems, or pillars: the information transport system (ITS), the Voice Switching System (VSS), the Net Battle Management/Net Defense (NBM/ND) system, and the Telecommunications Management System (TMS). All these assets combine to provide inter-base connectivity to link in-garrison command and control (C2) and combat support systems to the Defense Information System Network (DISN) utilizing NIPRNET and SIPRNET connectivity.

Client/server—A network application architecture which separates the client (usually the graphical user interface) from the server. Each instance of the client software can send requests to a server or application server.

Client Support Administrator (CSA)—Person who ensures functional communities of interest systems, servers, workstations, peripherals, communications devices, and software are on-line and supported.

Computer—A device or machine for making calculations or controlling operations that are expressible in numerical or logical terms.

Computer Network—A system for communication among two or more computers. These networks may be fixed (cabled, permanent) or temporary (as via modems).

Computer Program—An example of computer software that prescribes the actions ("computations") that are to be carried out by a computer.

Database—A collection of information stored in a computer in a systematic way, such that a computer program can consult it to answer questions.

Excess Equipment—An item is considered excess when it is no longer required due to mission change, equipment upgrades, technology changes, obsolescence, etc. The item is also considered excess when the total quantity on hand exceeds the required quantity, as identified in the technical solution/requirements document, plus the number of authorized spares as identified in the Logistics Support Plan.

Foreign National (FN)—Individual who is not a US citizen including US military personnel, DOD employees and contractors that are governed by the host nation Status of Forces Agreement (SOFA).

Global Information Grid (GIG)—The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel.

Mean Time Between Failure (MTBF)—For a particular interval, the total functional life of a population of an item divided by the total number of failures within the population. The definition holds for time, rounds, miles, events, or other measures of life unit. A basic technical measure of reliability.

Network Professional—Military, DOD civilian, contractor, or local national who fill a crew position in accordance with AFI 33-115, Volume 1, criteria. These individuals have been trained and certified to verifiable skill levels. They actively manage, configure and control the network and ensure DOD Information Assurance posture is maintained.

Operational Spare—An operational spare is a piece of serviceable equipment required to sustain operations in the interval between ordering and replenishment.

Order and Shipping Time (O&ST)—The time elapsing between the initiation of stock replenishment action for a specific activity and the receipt by that activity of the materiel resulting from such action. Order and shipping time is applicable only to materiel within the supply system, and it is composed of the distinct elements, order time, and shipping time. See also level of supply.

Reliability—The ability of a system and its parts to perform its mission without failure, degradation, or demand on the support system. See Mean Time Between Failure (MTBF).

Single Point Failure (SPF) Items—Single point failure items are items whose failure will render a system inoperative and/or unable to perform its designated mission. Also can be described as *any* part of the system that can, if it fails, cause an interruption of required service from that system. This can be as simple as a process failure or as catastrophic as a computer system crash.

Attachment 2

SERVICE LEVEL AGREEMENT, MEMORANDUM OF AGREEMENT, MEMORANDUM OF UNDERSTANDING

A2.1. Sample. The following is a sample of a SLA, MOA/MOU format between the service provider and the customer. The sample agreement shows only minimum topics that should be addressed; however, ensure the chosen document covers NCC Core Services (see **Chapter 6**).

1. Introduction. Parties (organizations) involved:
    a. Service provider: (i.e., DAA or NCC).
        (1) POC names.
        (2) Location or office symbol.
        (3) Telephone numbers.
    b. End-user organization.
        (1) POC names.
        (2) Location or office symbols.
        (3) Telephone numbers
2. Purpose. The purpose of this document is to state the relationship between the service provider and the end-user organization. It specifies the services and commitments of the NCC as well as the expectations and obligations of the end-user organization.
3. Responsibilities of Service Provider (Name of the Organization). The service provider agrees that they will:
    a. Specify what resources they will use.
    b. Describe how they will inform the customer of infrastructure changes and new or changed service.
    c. State security methods that they will use to protect infrastructure resources from unauthorized access, monitoring, or tampering.
    d. Describe process used to notify and coordinate with end-user organization about planned outages of connectivity, equipment, or electricity.
    e. Explain the coordination process for service degradation or failure correction and state how customer will be kept informed of status.
    f. Describe materials that will be provided to customer to minimize procedural errors.
    g. Explain customer support performance criteria and workload limitations (e.g., hours of operation, response times, and expected maximum calls).
    h. Describe what performance data and analysis reports they will provide to the customer organization to show service quality and level of customer support provided.

i. State what customer training is available and what role the service providers will play in customer training.

j. Perform periodic surveys to monitor customer satisfaction.

k. State the security measures they will use to protect infrastructure resources from unauthorized access, monitoring, or tampering.

4. Responsibilities of End-User Organization.

a. The end-user organization agrees that it will:

(1) Describe the process used to ensure end-users know procedures for getting help.

(2) Coordinate with service provider on any planned and in-progress major configuration changes (e.g., network installation/expansion, TCP/IP port requirements, changes in topology, system upgrades, relocation, etc.).

(3) CSAs and SAs will provide, upon request, equipment layout, network schematic, network connectivity (attached via backbone or stand alone), and their exact location.

(4) Describe how they will use the performance and trend analysis data from service provider and provide feedback to improve service.

(5) Develop end-user contingency operations plans and capabilities.

(6) Identify what resources they will matrix or transfer to the service provider.

(7) Provide service provider with access to equipment both electronically and physically as needed.

(8) Agree to perform the certification effort and comply with wing or NCC security policy.

(9) Coordinate with the service provider at least annually to discuss changes in service levels and SLAs.

(10)Support the resourcing of IT necessary to meet agreed SLAs, MOAs/MOUs. If IT cannot be resourced adequately, adjust levels downward sufficiently to ensure they can be met by the expected resource levels.

(11)Annually review the IT restoration priorities. Update missions, functions, and systems requiring IT support to ensure all IT has the restoration priority necessary to meet mission needs.

b. During a trouble call, the end users will:

(1) Contact organization’s CSA first, if available.

(2) Describe what minimum information they will provide (e.g., name, organization, location, telephone number, equipment number, user-id, E-mail address).

(3) Provide service provider with a description of problem, its priority, and potential mission impact.

(4) Work with the service provider during fault isolation process, as needed.

(5) Negotiate for increased workload/expansion for contingencies or new support.

5. Customer Escalation Procedures. The two parties agree to the following procedures in case they need to escalate resolution of the problem (e.g., when the customer is not satisfied with the service provided).

   a. Escalation Levels, To Whom, and Phone Numbers.

      (1) 1st

      (2) 2nd

      (3) 3rd

6. Conclusion.

   a. Parties agree that the terms of this agreement will remain in effect for (5 years, 6 months, etc.) and are subject to review (annually, semiannually, etc.).

   b. The parties agree to the following mechanism for initiating an out-of-cycle SLA, MOA/MOU review:

   c. Service levels and procedures established herein were agreed to by parties represented by the undersigned.

_____________________________________ __________________________________

(Service Provider Representative Signature) (End-User Organization Signature)

Attachments (add as needed):

1. Hours of Operation
2. Definitions of Terminology
3. Lists of Support Equipment and Software
4. Summaries of Applicable Contracts
5. Contingency Plan

Attachment 3

CREW POSITIONS

A3.1. General. This attachment identifies the crew positions located at each network operations level. **Table A3.1.** illustrates the relationship between tiered-level crew positions and specific NETOPS Mission Areas. Crew positions are grouped into three functional areas. These areas are Information Protection Operations (IPO), Network Management (NM), and Network Administration (NA).

A3.2. Functional Area Descriptions.

A3.2.1. Network Administration (NA) Positions. This functional area is responsible for central management of server hardware, operating systems and applications. Responsibilities include some of the core services (as outlined in **Chapter 6**) provided by the NOSC/NCC to the base or MAJCOM populace. The individuals assigned to this functional area are the base experts in system administration and also provide technical assistance to FSAs and CSAs who provide administration support from their servers to their end-user workstations. NA positions are divided into three positions: Configuration Management Technician, Application Services Technician, and Messaging Technician. Network Administration personnel function at the IT-1 (DODI 8500.2, *Information Assurance (IA) Implementation*) and ADP-1 (DOD 5200.2-R, *Personnel Security Program*) level.

A3.2.2. Network Management (NM) Positions. This functional area provides proactive and reactive management of resources by monitoring and controlling the network infrastructure, available bandwidth, hardware, and distributed software resources. Responsibilities include some of the core services (as outlined in **Chapter 6**) provided by the NOSC/NCC to the base or MAJCOM populace. NM responds to detected security incidents, network faults (errors) and user reported outages. NM is further divided into two positions: Infrastructure Technician and Network Services Technician. Network Management personnel function at the IT-1 (DODI 8500.2) and ADP-1 (DOD 5200.2-R) level.

A3.2.3. Information Protection Operations (IPO) Positions. This functional area implements and enforces national, DOD, and Air Force security policies and directives. It provides proactive security functions established to assist Air Force organizations in deterring, detecting, isolating, containing, and recovering from information system (IS) and network security intrusions. This area conducts IPO employing hardware and software tools to enhance the security of their networks. The personnel in this area install, monitor, and direct proactive and reactive network information protection defensive measures to ensure the availability, integrity, and reliability of base networked and stand-alone information resources. Information Protection Operations are divided into three crew positions: Boundary Protection Specialist, Intrusion Detection Specialist, and Vulnerability Assessment Specialist. Information Protection Operations personnel function at the IT-1 (DODI 8500.2) and ADP-1 (DOD 5200.2-R) level.

A3.3. Unit Level Positions.

A3.3.1. Client Support Administrator (CSA). CSAs serve as the first line of help to resolve customers' administrative and technical problems. CSAs are usually not assigned to the NCC, though are logically an extension of the Help Desk team. CSAs take direction from the NCC and FSA. NCC direction takes precedence over FSA direction. CSAs install, configure, and operate client/server devices. The CSA will be a 3A0X1 unless mission requirements exceed available manning. When a 3A0X1 is not assigned, any AFSC or occupational series can perform CSA duties once trained and certified. CSAs function at the IT-2 (DODI 8500.2) and ADP-2 (DOD 5200.2-R) level.

A3.4. Network Control Center (NCC) and Network Operations and Security Center (NOSC) Crew Positions.

A3.4.1. Configuration Management Technician. Installs and configures the network operating system for all servers to Air Force specifications. Establishes print services and maintains standardized file storage directory structures. Creates user accounts in accordance with Air Force standard naming conventions and provides file, print, and messaging access. Maintains directory services supporting the Air Force Directory, performs preventive maintenance and ensures data recovery capability through proper data backup scheduling and execution.

A3.4.2. Application Services Technician. Installs, configures, operates, and maintains network-launched user applications and the trouble ticketing system and its database.

A3.4.3. Messaging Technician. Installs, configures, operates, and maintains network messaging applications. Maintains accuracy of the Global Address List (GAL) as well as local address lists supporting the Air Force Directory and Air Force White Pages.

A3.4.4. Network Services Technician. Maintains the NM systems to include backup of these systems. They are responsible for collecting and archiving the data necessary to conduct detailed infrastructure mapping and analysis, producing time-sensitive displays and threshold alerts, and developing course of action scenarios. Controls all base IP address space through use of DHCP, or static configuration. Maintains DNS servers for internal and external name resolution.

A3.4.5. Infrastructure Technician. Modifies switch, router, and hub configurations to ensure optimum network performance. Configures access control lists to grant/restrict network access to authorized users and processes. Uses approved NM software and tools to perform their tasks. Infrastructure technicians are experts in operating and configuring routers and switches, in addition to a variety of hubs and transmission media.

A3.4.6. Intrusion Detection Specialist. Uses Air Force standard automated security tools to deter, detect, isolate network intrusions, and recover compromised systems after attack.

A3.4.7. Vulnerability Assessment Specialist. Performs internal network security assessments, using Air Force standard automated security tools to minimize and/or eliminate threat of network intrusion by proactively probing network defenses to identify vulnerabilities. Ensures systems are compliant with TCNO requirements and updates/reports status. Determines and reports the information protection posture of the base network. Ensures all current network security tools and patches are implemented across all internal base systems. Base will maintain ability to monitor, detect, analyze, summarize, report, control, isolate, contain, recover and correct vulnerabilities.

A3.4.8. Boundary Protection Specialist. Installs, configures, and maintains the CITS IA suite. Operates and maintains firewall(s), web proxy and caching servers, and E-mail gateway server to protect base information resources from internal and external threats.

A3.5. Air Force Network Operations and Security Center (AFNOSC) and Network Operations and Security Center (NOSC) Positions.

A3.5.1. Network Defense Controller. Network defense controllers oversee intrusion detection, boundary protection and vulnerability assessment operations to defend the AF-GIG. Network defense controllers develop a network defense visibility display, direct time sensitive adjustments to the network security posture to minimize or counter operational risk, and collect and store the data and metrics necessary to conduct Operational Risk Management (ORM). They also direct security measures such as identification/authentication controls, internal encryption, and intrusion detection for the NOSC or NCCs under their control. Network Defense Controllers function at the IT-1 (DOD 8500.2) and ADP-1 (DOD 5200.2-R) level.

A3.5.2. Enterprise Controller. Enterprise Controllers oversee network administration and network management operations for the AF-GIG. They are responsible for monitoring network management software and generating ad hoc queries for network assistance, and directing courses of action. Enterprise controllers maintain a “watch” on network performance characteristics and infrastructure centers of gravity, and recommend adjustments. They centrally monitor server, user, and server-launched applications to ensure efficient use. They also create and report appropriate metrics within their area of responsibility. Enterprise Controllers function at the IT-1 (DOD 8500.2) and ADP-1 (DOD 5200.2-R) level

A3.5.3. Voice Controller. Voice Controllers are responsible for operating, managing, and maintaining the ETM platform and help provide situational awareness of all MAJCOM voice networks (e.g., DSN, public switched telephone network, and Federal Telecommunications System 2001). Voice Controllers develop VPS security policies, custom report development, recurring and ad-hoc report generation, moves/adds/changes associated with VPS policy, troubleshooting and system maintenance, upgrades system backups, and regular administrative reporting. They are also responsible for coordinating VPS-related issues with individual bases. Voice Controllers function at the IT-1 (DOD 8500.2) and ADP-1 (DOD 5200.2-R) level.

A3.6. Crew Positions at All Levels.

A3.6.1. Crew Commander. Crew Commander is the only officer crew position. They serve at all three levels of NETOPS hierarchy--the AFNOSC, NOSC, and NCC. NCCs with limited manning may utilize Operations Controllers in place of Crew Commanders. Responsibilities include successful mission execution, maintaining crew integrity, and ensuring crew members are trained and certified. Crew Commanders conduct changeover briefings and prepare daily standup briefings. They coordinate with wing/base-level Operations Security (OPSEC) and counterintelligence (AFOSI) personnel on defense counter-information (DCI) plans/operations, and deconflict NetD activities with on-going aerospace operations and missions. Additionally, they maintain daily logs, coordinate with external customers, and review SITREPs, OPREP3s, INFOCONs, TCNOs, and C4 NOTAMs. Crew commanders maintain restoration and recovery plans and procedures and ensure positive control over network defense operations. In short, they maintain tactical and operational control over their assigned crew.

A3.6.2. Operations Controller. Operations controllers serve at each tier of the network operations hierarchy. They are required at the AFNOSC and NOSC, but optional at the NCC. The operations controller cannot be dual hatted with another crew position (e.g., they cannot fill an enterprise controller position and operations controller position during the same shift). Operations controllers are seasoned network professionals (preferably a senior NCO) and certified in at least one crew position. They are the right-hand of the crew commander. They advise crew commanders of critical situations and recommend courses of action. Additionally, they help maintain daily logs, and review SITREPs, OPREP3s, INFOCONs, TCNOs, and C4 NOTAMs. Operations controllers help crew commander ensure positive control over their assigned crew.

A3.6.3. Help Desk Technician/Event Manager. Help Desk technicians are in essence event managers. At the NCC level Help Desk technicians are the CSA and FSA point of contact to the NCC. They utilize a standard trouble ticketing database for inputting, assigning, resolving and closing trouble tickets. Event managers are responsible for maintaining a real-time view of the base network, theater network, or AF-GIG ability to perform its designed functions. Event managers also prepare monthly metrics showing operational performance. Help Desk technicians and event managers must be certified in at least one crew position. Helpdesk/Event Managers function at the IT-1 (DOD 8500.2) and ADP-1 (DOD 5200.2-R) level.

Table A3.1. Network Operations Mission Areas.

				Systems and Network Management	Information Dissemination Management	Information Assurance
CREW POSITIONS	UNIT		Functional Systems Administrator			
			Client Support Administrator			
	NCC		Event Manager/Help Desk			
		Network Admin Positions	Configuration Management Technician			
			Application Services Technician			
			Messaging Technician			
		Information Protection	Boundary Protection Specialist			
			Intrusion Detection Specialist			
			Vulnerability Assessment Specialist			
		Network Mgt	Infrastructure Technician			
			Network Services Technician			
			Operations Controller			
			Crew Commander			
	NOSC		Network Defender			
		Information Protection Operations	Boundary Protection Specialist			
			Intrusion Detection Specialist			
			Vulnerability Assessment Specialist			
			Enterprise Controller			
		Network Admin Positions	Configuration Management Technician			
			Application Services Technician			
			Messaging Technician			

Network Operations Mission Areas					
CREWPOSITIONS			Systems and Network Management	Information Dissemination Management	Information Assurance
	AFNOSC	Network Defense Controller			
		Enterprise Controller			
		Event Manager/Help Desk			
		Operations Controller			
		Crew Commander			

Table Key:Shading indicates under consideration for each table entry.

Attachment 4

VULNERABILITY ASSESSMENT SPECIALIST APPOINTMENT AND KEY REPLACEMENT REQUEST

A4.1. Vulnerability Assessment Specialist (VAS) Appointment and Key Replacement Request. This attachment is an example of a VAS appointment and Vulnerability Assessment Tool (VAT) key replacement request.

MEMORANDUM FOR HQ SSG/SWSN (CITS ENSC ISS KEY AGENT)

FROM: 2004 CS/SC

SUBJECT: Vulnerability Assessment Specialist (VAS) Appointment and Vulnerability Assessment Tool (VAT) Key Replacement Request

1. The below individual is appointed as the VAS for ____________________ AFB:

Rank/Name:	
Office Symbol:	
Phone Number:	
E-mail Address:	
ISS Training Info:	
Training Date:	
Affidavit:	I will use ISS for official government purposes only on the _______________ AFB network or _________ network according to the Internal Control Tools (ICT) as published in Air Force approved publication or message. ________________________________ APPOINTEE SIGNATURE

2. The above appointed person will use this memorandum, formal ISS training completion, and the domain-specific ISS key as their authority to run ISS on our network. Request ISS key be shipped to the below address:

Request Type:	[Initial -or- Replacement]
Specify ISS key IP Address Range(s):	xxx.yy.0.0 - xxx.yy.255.255 **(Example)**
Complete Mailing Address:	[Provide the complete ISS/VAS Operator name and mailing address, including building and room number]

3. The ISS POC is ____________________________ DSN ____________.

JOHN E. DOE, Major, USAF

Commander

cc: VAS Appointee